kaspersky

Kaspersky Endpoint Security für Windows 11.6.0

Inhalt

Häufige Fragen

ALLGEMEIN

SOFTWARE-VERTEILUNG

UPDATE

SICHERHEIT

INTERNET

PROGRAMMMODULE

GERÄTE

VERSCHLÜSSELUNG

SUPPORT

Wie wird Kaspersky Endpoint Security davor geschützt, vom Benutzer entfernt zu werden?	Wie wird eine Ablaufverfolgungsdatei erstellt? Wie wird die Dump-Aufzeichnung aktiviert?

Neuerungen

Update 11.6.0

Kaspersky Endpoint Security 11.6.0 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Unterstützung für Windows 10 21H1. Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10 finden Sie in der Wissensdatenbank des Technischen Supports.

2. Die Komponente "Managed Detection and Response" wurde hinzugefügt. Diese Komponente erleichtert die Interaktion mit der Lösung, die als "Kaspersky Managed Detection and Response" bekannt ist. *Kaspersky Managed Detection and Response (MDR)* bietet rund um die Uhr Schutz vor stetig zunehmenden Bedrohungen, die automatisierte Schutzmechanismen von Unternehmen umgehen können. Solche Mechanismen werden häufig von Unternehmen eingesetzt, die Schwierigkeiten haben, hochqualifizierte Experten zu finden, oder über begrenzte interne Ressourcen verfügen. Ausführliche Informationen zur Funktionsweise der Lösung *finden Sie in der Hilfe zu Kaspersky Managed Detection and Response*.

3. Das Programm Kaspersky Endpoint Agent, das zum Lieferumfang gehört, wurde auf Version 3.10 aktualisiert. In Kaspersky Endpoint Agent 3.10 wurden neue Funktionen eingeführt, einige frühere Probleme behoben und die Stabilität verbessert. Weitere Informationen zum Programm finden Sie in der Dokumentation zu Kaspersky-Lösungen, die Kaspersky Endpoint Agent unterstützen.

4. Jetzt kann der Schutz vor Angriffen wie Network Flooding und Portscanning in den Einstellungen des "Schutzes vor Netzwerkbedrohungen" verwaltet werden.

5. Neue Methode zum Erstellen von Netzwerkregeln für die Firewall wurden hinzugefügt. Sie können Paketregeln und Programmregeln für Verbindungen hinzufügen, die im Fenster Netzwerkmonitor angezeigt werden. Die Einstellungen für Verbindungen gemäß den Netzwerkregeln werden jedoch automatisch konfiguriert.

6. Die Benutzeroberfläche des Netzwerkmonitors wurde verbessert. Informationen über die Netzwerkaktivität wurden hinzugefügt: ID des Prozesses, der die Netzwerkaktivität initiiert; Netzwerktyp (lokales Netzwerk oder Internet); lokale Ports. Die Informationen über den Netzwerktyp sind standardmäßig ausgeblendet.

7. Es ist nun möglich, automatisch Benutzerkonten des Authentifizierungsagenten für neue Windows-Benutzer zu erstellen. Mithilfe des Agenten können Benutzer die Authentifizierung für den Zugriff auf Datenträger durchlaufen, die mit der Technologie "Kaspersky-Festplattenverschlüsselung" verschlüsselt wurden, und das Betriebssystem laden. Das Programm überprüft Informationen zu Windows-Benutzerkonten auf dem Computer. Wenn Kaspersky Endpoint Security ein Windows-Benutzerkonto erkennt, das kein Benutzerkonto des Authentifizierungsagenten besitzt, erstellt das Programm ein neues Konto für den Zugriff auf verschlüsselte Laufwerke. Es ist also nicht erforderlich, für Computer mit bereits verschlüsselten Laufwerken Authentifizierungsagenten-Benutzerkonten manuell hinzuzufügen.

8. Es ist nun möglich, den Vorgang der Festplattenverschlüsselung in der Programmoberfläche auf den Computern der Benutzer zu überwachen (Kaspersky Disk Encryption und BitLocker). Das Tool "Encryption Monitor" kann über das Programmhauptfenster ausgeführt werden.

Update 11.5.0

Kaspersky Endpoint Security 11.6.0 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Unterstützung für Windows 10 20H2. Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10 finden Sie in der Wissensdatenbank des Technischen Supports.

2. Aktualisierte Programmoberfläche. Außerdem wurde das Programmsymbol im Infobereich, in den Programmbenachrichtigungen und in den Dialogfeldern aktualisiert.

3. Verbesserte Schnittstelle des Web-Plug-Ins von Kaspersky Endpoint Security für die Komponenten Application Control, Device Control und Adaptive Anomaly Control.

4. Funktionen zum Importieren und Exportieren von Listen von Regeln und Ausnahmen im XML-Format hinzugefügt. Mit dem XML-Format können Sie Listen nach dem Export bearbeiten. Sie können Listen nur in der Konsole von Kaspersky Security Center verwalten. Die folgenden Listen stehen für den Export/Import zur Verfügung:

   - Verhaltenserkennung (Liste der Ausnahmen).
   - Schutz vor Web-Bedrohungen (Liste der vertrauenswürdigen Web-Adressen).
   - Schutz vor E-Mail-Bedrohungen (Liste der Erweiterungen für die Anlagenfilterung).
   - Schutz vor Netzwerkbedrohungen (Liste der Ausnahmen).
   - Firewall (Liste der Netzwerk-Paketregeln).
   - Programmkontrolle (Liste der Regeln).
   - Web-Kontrolle (Liste der Regeln).
   - Überwachung von Netzwerkports (Listen von Ports und Programme, die von Kaspersky Endpoint Security überwacht werden).
   - Kaspersky-Festplattenverschlüsselung (Liste der Ausnahmen).
   - Wechseldatenträger verschlüsseln (Liste der Regeln).

5. Dem Bericht über die Erkennung von Bedrohungen wurden MD5-Informationen zum Objekt hinzugefügt. In früheren Versionen des Programms zeigte Kaspersky Endpoint Security nur den SHA256 eines Objekts an.

6. Es wurde die Möglichkeit hinzugefügt, die Priorität für Geräte-Zugriffsregeln in den Einstellungen für die Gerätekontrolle zuzuweisen. Die Prioritätszuweisung ermöglicht eine flexiblere Konfiguration des Benutzerzugriffs auf Geräte. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Beispielsweise können Sie der Gruppe "Jeder" schreibgeschützte Leseberechtigungen und der Gruppe "Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 0 und für die Gruppe "Jeder" eine Priorität von 1 zu. Sie können die Priorität nur für Geräte konfigurieren, die über ein Dateisystem verfügen. Dazu gehören Festplatten, Wechsellaufwerke, Disketten, CD/DVD-Laufwerke und tragbare Geräte (MTP).

7. Neue Funktionalität hinzugefügt:

   - Audiobenachrichtigungen verwalten.
   - Kostenbewusstes Networking. Kaspersky Endpoint Security begrenzt den eigenen Netzwerkverkehr, wenn die Internetverbindung eingeschränkt ist (z. B. durch eine mobile Verbindung).
   - Verwalten Sie die Einstellungen von Kaspersky Endpoint Security über vertrauenswürdige Remote-Verwaltungsprogramme (wie TeamViewer, LogMeIn Pro und Remotely Anywhere). Mit Programmen zur Remote-Verwaltung können Sie Kaspersky Endpoint Security starten und Einstellungen in der Programmoberfläche verwalten.
   - Verwalten Sie die Einstellungen für die Untersuchung von sicherem Datenverkehr in Firefox und Thunderbird. Sie können den Zertifikatspeicher auswählen, der von Mozilla verwendet wird: den Windows-Zertifikatspeicher oder den Mozilla-Zertifikatspeicher. Diese Funktionalität steht nur für Computer zur

Verfügung, die über keine angewandte Richtlinie verfügen. Wenn eine Richtlinie auf einen Computer angewendet wird, ermöglicht Kaspersky Endpoint Security automatisch die Verwendung des Windows-Zertifikatspeichers in Firefox und Thunderbird.

8. Es wurde die Möglichkeit hinzugefügt, den Untersuchungsmodus für den sicheren Datenverkehr zu konfigurieren: Datenverkehr immer untersuchen, auch wenn Schutzkomponenten deaktiviert sind, oder Datenverkehr untersuchen, wenn dies von Schutzkomponenten angefordert wird.

9. Überarbeitetes Verfahren zum Löschen von Informationen aus Berichten. Ein Benutzer kann nur alle Berichte löschen. In früheren Versionen des Programms konnte ein Benutzer bestimmte Programmkomponenten auswählen, deren Informationen aus den Berichten gelöscht werden würden.

10. Überarbeitetes Verfahren zum Importieren einer Konfigurationsdatei, die Kaspersky Endpoint Security-Einstellungen enthält, und überarbeitetes Verfahren zur Wiederherstellung von Programmeinstellungen. Vor dem Importieren oder Wiederherstellen zeigt Kaspersky Endpoint Security lediglich eine Warnung an. In früheren Versionen des Programms konnten Sie die Werte der neuen Einstellungen anzeigen, bevor sie angewendet wurden.

11. Vereinfachtes Verfahren zur Wiederherstellung des Zugriffs auf ein Laufwerk, das mit BitLocker verschlüsselt wurde. Nach Abschluss des Zugriffswiederherstellungsverfahrens fordert Kaspersky Endpoint Security den Benutzer auf, ein neues Kennwort oder einen neuen PIN-Code festzulegen. Nachdem ein neues Kennwort festgelegt wurde, verschlüsselt BitLocker das Laufwerk. In der vorherigen Version des Programms musste der Benutzer das Kennwort in den BitLocker-Einstellungen manuell zurücksetzen.

12. Benutzer können jetzt ihre eigene lokale vertrauenswürdige Zone für einen bestimmten Computer erstellen. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen. Ein Administrator kann die Verwendung lokaler Ausnahmen oder lokaler vertrauenswürdiger Programme zulassen oder sperren. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

13. Es wurde die Möglichkeit hinzugefügt, Kommentare in die Eigenschaften von vertrauenswürdigen Programmen einzugeben. Kommentare tragen dazu bei, die Suche und Sortierung von vertrauenswürdigen Programmen zu vereinfachen.

14. Programmverwaltung über eine REST API:

    - Es gibt jetzt die Möglichkeit, die Einstellungen der Schutz vor E-Mail-Bedrohungen-Erweiterung für Outlook zu konfigurieren.

    - Es ist verboten, die Erkennung von Viren, Würmern und Trojanern zu deaktivieren.

Aktualisierung 11.4.0

Kaspersky Endpoint Security für Windows 11.4.0 bietet folgende Neuerungen und Verbesserungen:

1. Das Design des Symbols im Infobereich der Taskleiste wurde aktualisiert. Anstelle des Symbols wird jetzt das Symbol verwendet. Wenn der Benutzer eine Aktion ausführen muss (z. B. Neustart des Computers nach einem Programm-Update), ändert sich das Symbol in . Wenn die Funktion der Schutzkomponenten des Programms deaktiviert oder gestört ist, ändert sich das Symbol in oder . Wenn mit dem Mauszeiger auf das Symbol gezeigt wird, zeigt Kaspersky Endpoint Security eine Beschreibung des Problems an, das im Computerschutz vorliegt.

2. Das Programm Kaspersky Endpoint Agent, das zum Lieferumfang gehört, wurde auf Version 3.9 aktualisiert. Kaspersky Endpoint Agent 3.9 unterstützt die Integration mit neuen Kaspersky-Lösungen. Weitere Informationen zum Programm finden Sie in der Dokumentation zu Kaspersky-Lösungen, die Kaspersky Endpoint Agent unterstützen.

3. Der Status *Wird von der Lizenz nicht unterstützt* wurde für die Komponenten von Kaspersky Endpoint Security hinzugefügt. Den Status der Komponenten können Sie durch Klick auf **Schutzkomponenten** im Programmhauptfenster einsehen.

4. Zu den Berichten wurden neue Ereignisse über die Funktion der Komponente "Exploit-Prävention" hinzugefügt.

5. Die Treiber für die Verwendung der Kaspersky-Festplattenverschlüsselung werden automatisch zur Windows-Wiederherstellungsumgebung (WinRE, Windows Recovery Environment) hinzugefügt, wenn die Festplattenverschlüsselung gestartet wird. In der vorherigen Programmversion wurden die Treiber bei der Installation von Kaspersky Endpoint Security hinzugefügt. Durch das Hinzufügen von Treibern zur WinRE kann die Stabilität des Programms bei einer Betriebssystemwiederherstellung auf Computern erhöht werden, die durch die Technologie Kaspersky-Festplattenverschlüsselung geschützt sind.

Die Komponente "Endpoint Sensor" wurde aus dem Programm Kaspersky Endpoint Security entnommen. Sie können die Einstellungen für "Endpoint Sensor" weiterhin mithilfe der Richtlinie anpassen, wenn auf dem Computer das Programm Kaspersky Endpoint Security der Versionen 11.0.0 – 11.3.0 installiert ist.

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security für Windows (im Folgenden auch „Kaspersky Endpoint Security") bietet dem Computer einen komplexen Schutz vor unterschiedlichen Bedrohungsarten, Netzwerkangriffen und betrügerischen Angriffen.

Zum Schutz Ihres Computers verwendet Kaspersky Endpoint Security die folgenden Technologien zum Erkennen von Bedrohungen:

- **Maschinelles Lernen**. Kaspersky Endpoint Security verwendet ein Modell, das auf Machine Learning basiert. Dieses Modell wurde von Kaspersky entwickelt. Während seiner Verwendung erhält das Modell kontinuierlich aktualisierte Bedrohungsdaten von KSN und wird auf diese Weise trainiert.

- **Cloud-Analyse**. Kaspersky Endpoint Security erhält Bedrohungsdaten von Kaspersky Security Network. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen.

- **Experten-Analyse**. Kaspersky Endpoint Security verwendet Bedrohungsdaten, die von den Virenanalysten von Kaspersky hinzugefügt werden. Die Virenanalysten überprüfen manuell Objekte, deren Reputation nicht automatisch ermittelt werden kann.

- **Verhaltensanalyse**. Kaspersky Endpoint Security analysiert die Aktivität von Objekten in Echtzeit.

- **Automatische Analyse**. Kaspersky Endpoint Security erhält Daten von einem automatischen System zur Objektanalyse. Dieses System verarbeitet alle von Kaspersky empfangenen Objekte, ermittelt die Reputation der Objekte und erweitert die Antiviren-Datenbanken um die entsprechenden Daten. Ist das System nicht in der Lage, die Reputation eines Objekts zu ermitteln, so sendet es eine Anfrage an die Virenanalysten von Kaspersky.

- **Kaspersky Sandbox**. Kaspersky Endpoint Security untersucht Objekte auf virtuellen Maschinen. Kaspersky Sandbox analysiert das Verhalten von Objekten und fällt eine Entscheidung bezüglich dessen Reputation. Diese Technologie ist nur verfügbar, wenn Sie Kaspersky Sandbox nutzen.

Jeder Bedrohungstyp wird von einer bestimmten Programmkomponente verarbeitet. Die Komponenten können unabhängig voneinander aktiviert und deaktiviert sowie über ihre Einstellungen angepasst werden.

Die folgenden Programmkomponenten werden als Kontrollkomponenten bezeichnet:

- **Programmkontrolle**. Diese Komponente verfolgt den Start von Programmen durch den Anwender und reguliert den Programmstart.

- **Gerätekontrolle**. Diese Komponente ermöglicht es, flexible Zugriffsbeschränkungen einzurichten für Geräte, die als Informationsquellen dienen (z. B. Festplatten, Wechseldatenträger, CD/DVD-Disks), Datenübertragungsgeräte (z. B. Modems), Geräte für die Datenumwandlung (z. B. Drucker), oder Schnittstellen, mit deren Hilfe Geräte mit einem Computer verbunden werden können (z. B. USB und Bluetooth).

- **Web-Kontrolle**. Diese Komponente ermöglicht es, für verschiedene Anwendergruppen flexible Zugriffsbeschränkungen für Webressourcen einzurichten.

- **Adaptive Kontrolle von Anomalien**. Die Komponente überwacht und reguliert potentiell gefährliche Aktionen, die für den geschützten Computer nicht charakteristisch sind.

Die folgenden Programmkomponenten werden als Schutzkomponenten bezeichnet:

- **Verhaltensanalyse**. Diese Komponente erhält Daten über die Aktionen der Programme auf Ihrem Computer und versorgt die anderen Schutzkomponenten mit entsprechenden Informationen, um die Effektivität des Schutzes zu steigern.

- **Exploit-Prävention**. Diese Komponente verfolgt die ausführbaren Dateien, die von verwundbaren Programmen gestartet werden. Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer initiiert wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei.

- **Programm-Überwachung**. Diese Komponente registriert die Aktionen, die von Programmen im Betriebssystem ausgeführt werden, und reguliert die Aktionen von Programmen abhängig von der Gruppe, zu der ein Programm gehört. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln regulieren den Zugriff von Programmen auf persönliche Anwenderdaten sowie auf die Ressourcen des Betriebssystems. Zu solchen Daten zählen: Benutzerdateien im Ordner „Dokumente“, Cookies, Dateien mit einem Aktivitätsverlauf der Benutzers, sowie Dateien, Ordner und Registrierungsschlüssel, die Arbeitsparameter und wichtige Daten häufig verwendeter Programme enthalten.

- **Rollback von schädlichen Aktionen**. Mithilfe dieser Komponente kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

- **Schutz vor bedrohlichen Dateien**. Diese Komponente schützt das Dateisystem des Computers vor einer Infektion. Die Komponente nimmt sofort nach dem Start von Kaspersky Endpoint Security den Betrieb auf, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Massenspeichergeräten geöffnet, gespeichert und gestartet werden. Diese Komponente fängt jeden Zugriff auf eine Datei ab und untersucht diese Datei auf Viren und andere bedrohliche Programme.

- **Schutz vor Web-Bedrohungen**. Diese Komponente untersucht den Datenverkehr, der über die Protokolle HTTP und FTP auf dem Benutzercomputer empfangen wird. Außerdem überprüft sie, ob Webadressen als bösartig oder als Phishing gelten.

- **Schutz vor E-Mail-Bedrohungen**. Diese Komponente untersucht, ob in ein- und ausgehenden E-Mail-Nachrichten Viren und andere Schadprogramme enthalten sind.

- **Schutz vor Netzwerkbedrohungen**. Diese Komponente prüft den eingehenden Netzverkehr auf für Netzwerkangriffe charakteristische Aktivitäten. Wenn Kaspersky Endpoint Security einen Angriff auf den Computer erkennt, sperrt das Programm die Netzwerkaktivität des angreifenden Computers.

- **Firewall**. Diese Komponente gewährleistet den Schutz der Daten, die auf dem Benutzercomputer gespeichert sind. Während eine Verbindung zum Internet oder zum lokalen Netzwerk besteht, werden die meisten Bedrohungen blockiert, die das Betriebssystem gefährden können.

- **Schutz vor modifizierten USB-Geräten**. Diese Komponente verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem Computer verbunden werden.

- **AMSI-Schutz**. Die Komponente untersucht Objekte auf Anfrage von Dritthersteller-Anwendungen und informiert die Anwendung, von welcher die Anfrage stammt, über das Untersuchungsergebnis.

Zusätzlich zum konstanten Schutz, der anhand der Programmkomponenten realisiert wird, empfiehlt sich die regelmäßige Durchführung einer *Untersuchung des Computers* auf Viren und andere schädliche Programmen. Das ist erforderlich, um die Möglichkeit einer Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, da beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Um den Computerschutz stets auf dem neuesten Stand zu halten, ist ein *Update der im Programm verwendeten Datenbanken und Programm-Module* erforderlich. Standardmäßig wird das Programm automatisch aktualisiert. Bei Bedarf können Datenbanken und Programm-Module jedoch jederzeit manuell aktualisiert werden.

In Kaspersky Endpoint Security sind die folgenden Aufgaben vorgesehen:

- **Integritätsprüfung**. Kaspersky Endpoint Security überprüft, ob die Programm-Module, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Besitzt ein Programm-Modul eine inkorrekte digitale Signatur, so gilt das Modul als beschädigt.

- **Vollständige Untersuchung**. Kaspersky Endpoint Security führt eine Untersuchung des Betriebssystems aus und scannt dabei u. a. folgende Elemente: Kernel-Speicher, Objekte, die beim Start des Betriebssystems geladen werden, Bootsektoren, Sicherungsspeicher des Betriebssystems sowie sämtliche Festplatten und Wechseldatenträger.

- **Benutzerdefinierte Untersuchung**. Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte.

- **Untersuchung wichtiger Bereiche**. Kaspersky Endpoint Security untersucht den Kernel-Speicher, die Objekte, die beim Start des Betriebssystems geladen werden, und die Bootsektoren.

- **Update**. Kaspersky Endpoint Security lädt aktualisierte Datenbanken und Programm-Module. Dadurch befindet sich der Schutz des Computers vor Viren und anderen Schadprogrammen stets auf dem neuesten Stand.

- **Rollback des letzten Updates** Kaspersky Endpoint Security macht das letzte Update der Datenbanken und Programm-Module rückgängig. Dadurch besteht die Möglichkeit, bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückzukehren. Dies ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, welche dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert.

Verwaltungsfunktionen des Programms

Kaspersky Endpoint Security bietet mehrere Verwaltungsfunktionen. Die Verwaltungsfunktionen dienen dazu, das Programm auf dem neuesten Stand zu halten, die Optionen des Programms zu erweitern und den Benutzer zu unterstützen.

- **Berichte**. Während der Ausführung des Programms wird für jede Komponente ein Bericht erstellt. In den Berichten können Sie auch die Ausführungsergebnisse für Aufgaben verfolgen. Die Berichte enthalten Listen der Ereignisse, die während der Ausführung von Kaspersky Endpoint Security aufgetreten sind, sowie alle vom Programm ausgeführten Operationen. Treten Probleme auf, können Sie die Berichte an Kaspersky senden, um sie von den Experten des Technischen Supports eingehend untersuchen zu lassen.

- **Datenverwaltung**. Wenn das Programm bei der Untersuchung des Computers auf Viren und andere Schadprogramme infizierte Dateien findet, so werden diese Dateien blockiert. Kaspersky Endpoint Security speichert die Kopien desinfizierter und gelöschter Dateien im *Backup*. Dateien, die bisher nicht verarbeitet wurden, werden von Kaspersky Endpoint Security in die *Liste der aktiven Bedrohungen* verschoben. Sie können Dateien untersuchen, Dateien an ihrem ursprünglichen Speicherort wiederherstellen und die Datenverwaltung leeren.

- **Benachrichtigungsdienst**. Der Benachrichtigungsdienst ermöglicht dem Benutzer, die Ereignisse zu überwachen, die den Status des Computerschutzes und den Betrieb von Kaspersky Endpoint Security beeinflussen. Die Nachrichten können auf dem Desktop eingeblendet oder per E-Mail zugestellt werden.

- **Kaspersky Security Network**. Durch die Teilnahme des Anwenders an Kaspersky Security Network kann die Effizienz des Computerschutzes gesteigert werden, indem aktuelle Informationen zur Sicherheit und Zuverlässigkeit von Dateien, Webressourcen und Programmen von allen Teilnehmern weltweit verwendet werden.

- **Lizenz**. Durch den Kauf einer Lizenz erhalten Sie eine voll funktionsfähige Programmversion, Zugriff auf Updates für die Datenbanken und Programm-Module, sowie das Recht auf technischen Support bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail.

- **Support**. Alle registrierten Nutzer von Kaspersky Endpoint Security können sich im Falle eines Problems an unsere Experten vom Technischen Support wenden. Sie können aus dem Portal Kaspersky CompanyAccount eine Anfrage an den Technischen Support von Kaspersky senden oder die Hotline des Technischen Supports nutzen.

Wenn im Programm Fehler auftreten oder das Programm hängen bleibt, kann sich das Programm automatisch neu starten.

Treten bei der Ausführung des Programms wiederholt Fehler auf, aufgrund derer das Programm beendet wird, führt das Programm die folgenden Aktionen aus:

1. Deaktivierung der Schutz- und Überwachungsfunktionen (die Verschlüsselungsfunktion bleibt aktiv).
2. Benachrichtigung des Benutzers über die Deaktivierung der Funktionen.
3. Versuch der Wiederherstellung der Funktionsfähigkeit nach Updates der Antiviren-Datenbanken und der Übernahme von Updates der Programm-Module.

Lieferumfang

Zum Lieferumfang gehören die folgenden Programmpakete:

- **Strong encryption (AES256)**

  Das Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) mit einer effektiven Schlüssellänge von 256 Bit realisieren.

- **Lite encryption (AES56)**

  Das Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 56 Bit realisieren.

Jedes Programmpaket enthält die folgenden Dateien:

`kes_win.msi`	Installationspaket für Kaspersky Endpoint Security.
`setup_kes.exe`	Dateien, die für die Installation des Programms mit allen verfügbaren Methoden erforderlich sind.
`kes_win.kud`	Datei zur Erstellung eines Installationspakets für Kaspersky Endpoint Security.
`klcfginst.msi`	Installationspaket des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security“ für Kaspersky Security Center
`bases.cab`	Dateien mit Update-Paketen, die bei der Programminstallation verwendet werden
`cleaner.cab`	Dateien für die Deinstallation von inkompatibler Software.
`incompatible.txt`	Datei mit einer Liste der inkompatiblen Software.
`ksn_<Sprach-ID>.txt`	Datei, in der Sie die Bedingungen für die Teilnahme an Kaspersky Security Network lesen können.
`license.txt`	Datei, die den Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie enthält.
`installer.ini`	Datei, die interne Parameter des Programmpakets enthält.
`endpointagent.msi`	Installationspaket für das Programm Kaspersky Endpoint Agent Version 3.10, das für die Integration mit anderen Kaspersky-Lösungen erforderlich ist (z. B. mit Kaspersky Sandbox).
`NDP<Version>-<Paketeigenschaften>`	Installationspaket für Microsoft .NET Framework.

`keswin_web_plugin.zip`	Archiv, das die für die Installation des Web-Plug-ins von Kaspersky Endpoint Security erforderlichen Dateien enthält.

Es wird davon abgeraten, die Werte dieser Parameter zu ändern. Falls Sie die Installationseinstellungen ändern möchten, verwenden Sie die Datei setup.ini.

Hard- und Softwarevoraussetzungen

Um die Funktionsfähigkeit von Kaspersky Endpoint Security zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen.

Allgemeine Mindestanforderungen:

- 2 GB freier Speicherplatz auf der Festplatte
- PROZESSOR:
  - Workstation: 1 GHz
  - Server: 1,4 GHz
  - Unterstützung für den SSE2-Befehlssatz
- Arbeitsspeicher:
  - Workstation (x86): 1 GB
  - Workstation (x64): 2 GB
  - Server: 2 GB
- Microsoft .NET Framework 4.0 oder höher

Unterstützte Betriebssysteme für Workstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 und höher
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise.

Der Signaturalgorithmus des SHA-1-Moduls ist von Microsoft als veraltet eingestuft. Das Update KB4474419 ist für die erfolgreiche Installation von Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Microsoft Windows 7 erforderlich. Weitere Einzelheiten zu diesem Update finden Sie auf der Website des technischen Supports von Microsoft.

Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10 finden Sie in der Wissensdatenbank des Technischen Supports.

Unterstützte Betriebssysteme für Server:

- Windows Small Business Server 2011 Essentials / Standard (64-Bit)

  Microsoft Small Business Server 2011 Standard (64-Bit) wird nur unterstützt, wenn Service Pack 1 für Microsoft Windows Server 2008 R2 installiert ist.

- Windows MultiPoint Server 2011 (64-Bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 und höher
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter.

Der Signaturalgorithmus des SHA-1-Moduls ist von Microsoft als veraltet eingestuft. Das Update KB4474419 ist für die erfolgreiche Installation von Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Microsoft Windows Server 2008 R2 erforderlich. Weitere Einzelheiten zu diesem Update finden Sie auf der Website des technischen Supports von Microsoft.

Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows Server 2016 und Microsoft Windows Server 2019 finden Sie in der Wissensdatenbank des Technischen Supports.

Unterstützte Terminalserver-Typen:

- Microsoft Remote Desktop Services basierend auf Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services basierend auf Server 2012;
- Microsoft Remote Desktop Services basierend auf Windows Server 2012 R2;
- Microsoft Remote Desktop Services basierend auf Windows Server 2016;
- Microsoft Remote Desktop Services basierend auf Windows Server 2019.

Unterstützte virtuelle Plattformen:

- VMWare Workstation 16 Pro
- VMware ESXi 7.0 Update 1a
- Microsoft Hyper-V Server 2019

- Citrix Virtual Apps and Desktops 7
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security unterstützt die Verwendung der folgenden Versionen von Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B
- Kaspersky Security Center 13
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2

Vergleich der Programmfunktionen im Hinblick auf den Typ des Betriebssystems

Die Auswahl der für Kaspersky Endpoint Security verfügbaren Funktionen ist vom Typ des Betriebssystems abhängig: Workstation oder Server (siehe folgende Tabelle).

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Workstation	Server
Erweiterter Schutz		
Kaspersky Security Network	✓	✓
Verhaltensanalyse	✓	✓
Exploit-Prävention	✓	✓
Programm-Überwachung	✓	–
Rollback von schädlichen Aktionen	✓	✓
Basisschutz		
Schutz vor bedrohlichen Dateien	✓	✓
Schutz vor Web-Bedrohungen	✓	–
Schutz vor E-Mail-Bedrohungen	✓	–
Firewall	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓
Schutz vor modifizierten USB-Geräten	✓	✓
AMSI-Schutz	✓	✓

Sicherheitskontrolle		
Programmkontrolle	✓	✓
Gerätekontrolle	✓	–
Web-Kontrolle	✓	–
Adaptive Kontrolle von Anomalien	✓	–
Virtuelle Datentresore		
Kaspersky-Festplattenverschlüsselung	✓	–
BitLocker-Laufwerkverschlüsselung	✓	✓
Verschlüsselung von Dateien	✓	–
Wechseldatenträger verschlüsseln	✓	–
Endpoint Agent	✓	✓
Managed Detection and Response	✓	✓

Vergleich der Programmfunktionen in Abhängigkeit der Verwaltungs-Tools

Die Auswahl der verfügbaren Funktionen für Kaspersky Endpoint Security ist von den Verwaltungs-Tools abhängig (s. folgende Tabelle).

Sie können das Programm mithilfe der folgenden Konsolen für Kaspersky Security Center 12 verwalten:

- Verwaltungskonsole. Snap-In für Microsoft Management Console (MMC), das am Administrator-Arbeitsplatz installiert wird.
- Web Console. Komponente von Kaspersky Security Center, die auf dem Administrationsserver installiert wird. Mit der „Web Console“ können Sie über einen Browser auf einem beliebigen Computer arbeiten, der Zugriff auf den Administrationsserver besitzt.

Sie können das Programm auch mithilfe von Kaspersky Security Center Cloud Console verwalten. *Kaspersky Security Center Cloud Console* ist eine Cloud-Version von Kaspersky Security Center. In diesem Fall sind Administrationsserver und andere Komponenten von Kaspersky Security Center in einer Cloud-Infrastruktur von Kaspersky installiert. Details über die Programmverwaltung mithilfe von Kaspersky Security Center Cloud Console *finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console*.

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Kaspersky Security Center 12		Kaspersky Security Center
	Verwaltungskonsole	Web Console	Cloud Console
Erweiterter Schutz			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Verhaltensanalyse	✓	✓	✓
Exploit-Prävention	✓	✓	✓

Programm-Überwachung	✓	✓	✓
Rollback von schädlichen Aktionen	✓	✓	✓
Basisschutz			
Schutz vor bedrohlichen Dateien	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	✓
Firewall	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓
Schutz vor modifizierten USB-Geräten	✓	✓	✓
Managed Detection and Response	✓	✓	✓
AMSI-Schutz	✓	✓	✓
Sicherheitskontrolle			
Programmkontrolle	✓	✓	✓
Gerätekontrolle	✓	✓	✓
Web-Kontrolle	✓	✓	✓
Adaptive Kontrolle von Anomalien	✓	✓	✓
Virtuelle Datentresore			
Kaspersky-Festplattenverschlüsselung	✓	✓	–
BitLocker-Laufwerkverschlüsselung	✓	✓	✓
Verschlüsselung von Dateien	✓	✓	–
Wechseldatenträger verschlüsseln	✓	✓	–
Endpoint Agent	✓	✓	✓
Aufgaben			
Schlüssel hinzufügen	✓	✓	✓
Auswahl der Programmkomponenten ändern	✓	✓	✓
Inventarisierung	✓	✓	✓
Update	✓	✓	✓
Update-Rollback	✓	✓	✓
Virenuntersuchung	✓	✓	✓
Integritätsprüfung	✓	✓	–
Daten löschen	✓	✓	✓
Authentifizierungsagenten-Konten verwalten	✓	✓	–

Kompatibilität mit anderen Programmen

Kaspersky Endpoint Security überprüft vor der Installation, ob andere Kaspersky-Programme auf dem Computer vorhanden sind. Das Programm überprüft den Computer auch auf inkompatible Software. Eine Liste der inkompatiblen Software befindet sich in der Datei incompatible.txt, die zum Lieferumfang gehört.

INCOMPATIBLE.TXT-DATEI HERUNTERLADEN

Das Programm Kaspersky Endpoint Security ist nicht mit folgenden Kaspersky-Programmen kompatibel:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (einschließlich der Komponente „Endpoint Sensor“).
- Kaspersky Sandbox (einschließlich Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (einschließlich der Komponente „Endpoint Sensor“).

  Wenn die Komponente „Endpoint Agent“ mithilfe von Verteilungs-Tools für andere Kaspersky-Programme auf dem Computer installiert wurde, wird diese Komponente bei der Installation von Kaspersky Endpoint Security automatisch entfernt. Dabei kann es sein, dass Kaspersky Endpoint Security die Komponente „Endpoint Sensor“ / „Kaspersky Endpoint Agent“ enthält, falls Sie „Endpoint Agent“ in der Liste der Programmkomponenten ausgewählt haben.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security für Windows Server.
- Kaspersky Embedded Systems Security.

Falls auf dem Computer Kaspersky-Programme aus dieser Liste installiert sind, werden diese Programme durch Kaspersky Endpoint Security entfernt. Warten Sie bis zum Abschluss des Vorgang, um die Installation von Kaspersky Endpoint Security fortzusetzen.

Programm installieren und deinstallieren

Um das Programm Kaspersky Endpoint Security auf einem Computer zu installieren, gibt es folgende Möglichkeiten:

- lokal mithilfe des Installationsassistenten für das Programm.
- lokal aus der Befehlszeile
- per Fernzugriff mithilfe von Kaspersky Security Center 12.
- per Fernzugriff über den Gruppenrichtlinien-Editor von Microsoft Windows (Details finden Sie auf der *Website des Technischen Support von Microsoft*).
- per Fernzugriff mithilfe von System Center Configuration Manager

Es gibt mehrere Methoden, um die Einstellungen für die Programminstallation anzupassen. Falls Sie gleichzeitig mehrere Methoden für die Anpassung von Einstellungen verwenden, übernimmt Kaspersky Endpoint Security die Einstellungen mit der höchsten Priorität. Für die Prioritäten verwendet Kaspersky Endpoint Security die folgende Reihenfolge:

1. Einstellungen, die aus der Datei setup.ini stammen.
2. Einstellungen, die aus der Datei installer.ini stammen.
3. Einstellungen, die aus der Befehlszeile stammen.

Es wird empfohlen, vor Beginn der Installation von Kaspersky Endpoint Security (auch vor einer Remote-Installation) alle laufenden Programme zu schließen.

Software-Verteilung über Kaspersky Security Center 12

Es gibt mehrere Methoden, um Kaspersky Endpoint Security auf den Computern im Unternehmensnetzwerk zu verteilen. Sie können die für Ihr Unternehmen geeignete Verteilungsmethode auswählen oder mehrere Verteilungsmethoden gleichzeitig verwenden. Kaspersky Security Center 12 unterstützt die folgenden grundlegenden Verteilungsmethoden:

- Installation des Programms mithilfe des Softwareverteilungs-Assistenten.

  Die standardmäßige Installationsmethode bietet sich an, wenn die standardmäßigen Einstellungen von Kaspersky Endpoint Security für Sie passend sind und Ihr Unternehmen eine einfache Infrastruktur aufweist, die keine speziellen Einstellungen erforderlich macht.

- Installation des Programms mithilfe einer Aufgabe zur Remote-Installation.

  Diese universelle Installationsmethode erlaubt es, die Einstellungen von Kaspersky Endpoint Security anzupassen und die Aufgaben zur Remote-Installation flexibel zu verwalten. Die Installation von Kaspersky Endpoint Security besteht aus den folgenden Schritten:

  1. Erstellung eines Installationspakets;
  2. Erstellung einer Aufgabe zur Remote-Installation.

Kaspersky Security Center 12 unterstützt auch andere Methoden für die Installation von Kaspersky Endpoint Security, beispielsweise die Software-Verteilung im Rahmen eines Abbilds des Betriebssystems. Details über andere Methoden für die Software-Verteilung *finden Sie in der Hilfe zu Kaspersky Security Center 12*.

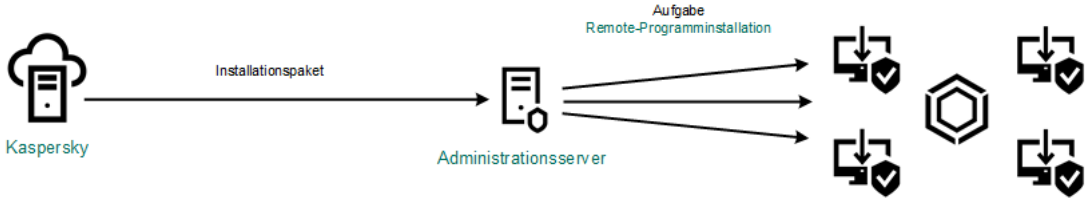
Standardmäßige Installation des Programms

Für die Programminstallation auf den Computern Ihres Unternehmens ist in Kaspersky Security Center ein Assistent für die Verteilung des Schutzes vorgesehen. Der Assistent für die Verteilung des Schutzes bietet die folgenden Basisaktionen:

1. Auswahl eines Installationspakets für Kaspersky Endpoint Security.

   Ein *Installationspaket* ist eine Auswahl von Dateien, welche mithilfe von Kaspersky Security Center für die Remote-Installation eines Kaspersky-Programms erstellt wird. Das Installationspaket enthält eine Auswahl von Einstellungen, welche für die Programminstallation erforderlich sind und die Funktionsfähigkeit direkt nach der Installation gewährleisten. Das Installationspaket wird auf Basis von Dateien mit den Erweiterungen kpd und kud erstellt, die zum Programmpaket gehören. Das Installationspaket für Kaspersky Endpoint Security ist für alle unterstützten Versionen des Betriebssystems Windows und Typen der Prozessorarchitektur gleich.

2. Erstellung der Aufgabe des Administrationsservers für Kaspersky Security Center *Remote-Programminstallation*.



Verteilung von Kaspersky Endpoint Security

Start des Assistenten für die Verteilung des Schutzes in der Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Erweitert → Remote-Installation**.

2. Klicken Sie auf den Link **Installationspakete auf den verwalteten Geräten (Arbeitsplätzen) verteilen**.

Dadurch wird der Sicherheits-Bereitstellungs-Assistent gestartet. Folgen Sie den Anweisungen.

Auf dem Client-Computer müssen die folgenden Ports geöffnet werden: TCP 139 und 445, UDP 137 und 138.

Schritt 1. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Zusammen mit Kaspersky Endpoint Security wird auch der Administrationsagent installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 2. Geräte für die Installation auswählen

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Einstellungen für die Aufgabe zur Remote-Installation festlegen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Wählen Sie die Mittel für die Programminstallation aus:
  - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.

- **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.

- **Durch Betriebssystemmittel mithilfe des Administrationsservers**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

- **Verhalten von Geräten, die von anderen Servern verwaltet werden**. Wählen Sie eine Installationsmethode für Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

- **Anwendung nicht installieren, wenn sie schon installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.

- **Installation des Administrationsagenten in Gruppenrichtlinien des Active Directory festlegen**. Manuelle Installation des Administrationsagenten mit Active Directory-Mitteln. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

Schritt 4. Lizenzschlüssel auswählen

Fügen Sie zum Installationspaket einen Schlüssel für die Programmaktivierung hinzu. Dieser Schritt ist optional. Falls sich auf dem Administrationsserver ein Lizenzschlüssel mit automatischer Verteilungsfunktion befindet, wird der Schlüssel später automatisch hinzugefügt. Außerdem können Sie das Programm später mithilfe der Aufgabe *Schlüssel hinzufügen* aktivieren.

Schritt 5. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 6. Inkompatible Programme vor der Programminstallation entfernen

Überprüfen Sie die Liste der inkompatiblen Programme und erlauben Sie die Deinstallation dieser Programme. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.

Schritt 7. Auswahl eines Benutzerkontos für den Zugriff auf Geräte

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 8. Installation starten

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe zur Remote-Installation nach Abschluss des Assistenten nicht starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Start des Assistenten für die Verteilung des Schutzes in „Web Console“ und „Cloud Console”

Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Gerätesuche und Verteilung → Verteilung und Zuweisung → Sicherheits-Bereitstellungs-Assistent** aus.

Dadurch wird der Sicherheits-Bereitstellungs-Assistent gestartet. Folgen Sie den Anweisungen.

Auf dem Client-Computer müssen die folgenden Ports geöffnet werden: TCP 139 und 445, UDP 137 und 138.

Schritt 1. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen. Um ein Installationspaket zu erstellen, ist es nicht erforderlich, das Programmpaket zu suchen und auf dem Computer zu speichern. In Kaspersky Security Center ist eine Liste der Programmpakete verfügbar, die sich auf den Kaspersky-Servern befinden, und die Erstellung des Installationspakets wird automatisch ausgeführt. Die Liste wird von Kaspersky aktualisiert, wenn neue Programmversionen erschienen sind.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Schritt 2. Lizenzschlüssel auswählen

Fügen Sie zum Installationspaket einen Schlüssel für die Programmaktivierung hinzu. Dieser Schritt ist optional. Falls sich auf dem Administrationsserver ein Lizenzschlüssel mit automatischer Verteilungsfunktion befindet, wird der Schlüssel später automatisch hinzugefügt. Außerdem können Sie das Programm später mithilfe der Aufgabe *Schlüssel hinzufügen* aktivieren.

Schritt 3. Administrationsagent auswählen

Wählen Sie die Version des Administrationsagenten aus, der zusammen mit Kaspersky Endpoint Security installiert werden soll. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 4. Geräte für die Installation auswählen

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 5. Erweiterte Einstellungen anpassen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Tool für die Programminstallation auswählen:
  - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.
  - **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.
  - **Durch Betriebssystemmittel mithilfe des Administrationsservers**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
- **Anwendung nicht installieren, wenn sie schon installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.
- **Installation des Installationspakets in Gruppenrichtlinien des Active Directory festlegen**. Die Installation von Kaspersky Endpoint Security wird manuell mit den Mitteln des Administrationsagenten oder mit den Mitteln von Active Directory ausgeführt. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

Schritt 6. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 7. Inkompatible Programme vor der Programminstallation entfernen

Überprüfen Sie die Liste der inkompatiblen Programme und erlauben Sie die Deinstallation dieser Programme. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.

Schritt 8. In eine Administrationsgruppe verschieben

Wählen Sie die Administrationsgruppe aus, in welche die Computer nach der Installation des Administrationsagenten verschoben werden sollen. Das Verschieben in eine Administrationsgruppe ist erforderlich, um Richtlinien und Gruppenaufgaben anzuwenden. Wenn ein Computer bereits zu einer Administrationsgruppe gehört, wird der Computer nicht mehr verschoben. Wenn Sie keine Administrationsgruppe auswählen, werden die Computer zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt.

Schritt 9. Benutzerkonto für den Zugriff auf Geräte auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 10. Installation starten

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Erstellung eines Installationspakets

Ein *Installationspaket* ist eine Auswahl von Dateien, welche mithilfe von Kaspersky Security Center für die Remote-Installation eines Kaspersky-Programms erstellt wird. Das Installationspaket enthält eine Auswahl von Einstellungen, welche für die Programminstallation erforderlich sind und die Funktionsfähigkeit direkt nach der Installation gewährleisten. Das Installationspaket wird auf Basis von Dateien mit den Erweiterungen kpd und kud erstellt, die zum Programmpaket gehören. Das Installationspaket für Kaspersky Endpoint Security ist für alle unterstützten Versionen des Betriebssystems Windows und Typen der Prozessorarchitektur gleich.

Erstellen eines Installationspakets in der Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Erweitert → Remote-Installation → Installationspakete**.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.

2. Klicken Sie auf **Installationspaket erstellen**.

Der Assistent zur Erstellung eines Installationspakets wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Typ des Installationspakets auswählen

Wählen Sie die Variante **Installationspaket für ein Kaspersky-Programm erstellen** aus.

Schritt 2. Namen des Installationspakets festlegen

Geben Sie einen Namen für das Installationspaket ein, z. B. `Kaspersky Endpoint Security für Windows 11.6.0`.

Schritt 3. Programmpaket für die Installation auswählen

Klicken Sie auf **Durchsuchen** und wählen Sie die Datei `kes_win.kud` aus, die zum Lieferumfang gehört.

Aktualisieren Sie bei Bedarf die Antiviren-Datenbanken im Installationspaket. Dazu dient das Kontrollkästchen **Updates aus der Datenverwaltung ins Installationspaket kopieren**.

Schritt 4. Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie

Lesen und akzeptieren Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie.

Das Installationspaket wird erstellt und zu Kaspersky Security Center hinzugefügt. Mithilfe des Installationspakets können Sie Kaspersky Endpoint Security auf den Computern des Unternehmensnetzwerks installieren oder die Programmversion aktualisieren. In den Einstellungen des Installationspakets können Sie auch die Programmkomponenten auswählen und die Einstellungen für die Programminstallation anpassen (s. Tabelle unten). Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Sie können die Datenbanken im Installationspaket aktualisieren, um das Volumen des Datenverkehrs beim Datenbanken-Update nach der Installation von Kaspersky Endpoint Security zu reduzieren.

Erstellen eines Installationspakets in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Gerätesuche und Verteilung → Verteilung und Zuweisung → Installationspakete** aus.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent zur Erstellung eines Installationspakets wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Typ des Installationspakets auswählen

Wählen Sie die Variante **Installationspaket für ein Kaspersky-Programm erstellen** aus.

Der Assistent erstellt ein Installationspaket aus dem Programmpaket, das sich auf den Kaspersky-Servern befindet. Die Liste wird automatisch aktualisiert, wenn neue Programmversionen erscheinen. Es wird empfohlen, für die Installation von Kaspersky Endpoint Security diese Variante auszuwählen.

Außerdem können Sie ein Installationspaket aus einer Datei erstellen.

Schritt 2. Installationspakete

Wählen Sie das Installationspaket für Kaspersky Endpoint Security für Windows aus. Der Vorgang zur Erstellung des Installationspakets wird gestartet. Während das Installationspaket erstellt wird, müssen die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie akzeptiert werden.

Das Installationspaket wird erstellt und zu Kaspersky Security Center hinzugefügt. Mithilfe des Installationspakets können Sie Kaspersky Endpoint Security auf den Computern des Unternehmensnetzwerks installieren oder die Programmversion aktualisieren. In den Einstellungen des Installationspakets können Sie auch die Programmkomponenten auswählen und die Einstellungen für die Programminstallation anpassen (s. Tabelle unten). Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Sie können die Datenbanken im Installationspaket aktualisieren, um das Volumen des Datenverkehrs beim Datenbanken-Update nach der Installation von Kaspersky Endpoint Security zu reduzieren.

Einstellungen des Installationspakets

Abschnitt	Beschreibung
Schutzkomponenten	In diesem Abschnitt können Sie die Programmkomponenten auswählen, die verfügbar sein sollen. Die Auswahl der Programmkomponenten können Sie später mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern* ändern. Die Komponenten „Schutz vor modifizierten USB-Geräten“ und „Endpoint Agent“ sowie die Komponenten zur Datenverschlüsselung werden standardmäßig nicht installiert. Diese Komponenten können in den Einstellungen des Installationspakets hinzugefügt werden.
Installationseinstellungen	**Pfad des Programms zur Umgebungsvariablen "%PATH%" hinzufügen**. Sie können den Installationspfad zur Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

Prozess für Programminstallation nicht schützen. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).

Kompatibilität mit Citrix PVS gewährleisten. Sie können die Unterstützung von Citrix Provisioning Services für die Installation von Kaspersky Endpoint Security auf einer virtuellen Maschine aktivieren.

Pfad des Ordners für die Programminstallation. Sie können den Installationspfad von Kaspersky Endpoint Security auf dem Client-Computer ändern. Das Programm wird standardmäßig im Ordner `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows` installiert.

Konfigurationsdatei. Sie können eine Datei laden, welche die Einstellungen für Kaspersky Endpoint Security vorgibt. Sie können eine Konfigurationsdatei auf der lokalen Programmoberfläche erstellen.

Datenbanken-Update im Installationspaket

Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Diese Datenbanken waren aktuell, als das Installationspaket erstellt wurde. Nach der Erstellung des Installationspakets können Sie die Antiviren-Datenbanken im Installationspaket aktualisieren. Dadurch lässt sich das Volumen des Datenverkehrs reduzieren, der beim Update der Antiviren-Datenbanken nach der Installation von Kaspersky Endpoint Security anfällt.

Um die Antiviren-Datenbanken in der Datenverwaltung des Administrationsservers zu aktualisieren, verwenden Sie die Administrationsserver-Aufgabe *Upload von Updates in den Speicher des Administrationsservers*. Details über das Update der Antiviren-Datenbanken in der Datenverwaltung des Administrationsservers finden Sie in der *Hilfe zu Kaspersky Security Center*.

Die Datenbanken in einem Installationspaket können nur in der Verwaltungskonsole und in Kaspersky Security Center 12 Web Console aktualisiert werden. Die Datenbanken in einem Installationspaket können nicht im Programm Kaspersky Security Center Cloud Console aktualisiert werden.

Über die Verwaltungskonsole (MMC) die Antiviren-Datenbanken im Installationspaket aktualisieren

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Erweitert** → **Remote-Installation** → **Installationspakete**.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.

2. Öffnen Sie die Eigenschaften des Installationspakets.

3. Klicken Sie im Abschnitt **Allgemein** auf **Datenbanken aktualisieren**.

Dadurch werden die Antiviren-Datenbanken im Installationspaket aktualisiert. Als Quelle dient die Datenverwaltung des Administrationsservers. Die Datei `bases.cab`, die zum Lieferumfang gehört, wird durch den Order `bases` ersetzt. In diesem Ordner werden die Daten der Update-Pakete abgelegt.

Über „Web Console“ die Antiviren-Datenbanken im Installationspaket aktualisieren

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Gerätesuche und Verteilung → Verteilung und Zuweisung → Installationspakete** aus.

   Eine Liste der in „Web Console“ geladenen Installationspakete geöffnet.

2. Klicken Sie auf den Namen des Installationspakets für Kaspersky Endpoint Security, in dem Sie die Antiviren-Datenbanken aktualisieren möchten.

   Das Eigenschaftenfenster für das Installationspaket wird geöffnet.

3. Klicken Sie auf der Registerkarte **Allgemeine Informationen** auf den Link **Datenbanken aktualisieren**.

Dadurch werden die Antiviren-Datenbanken im Installationspaket aktualisiert. Als Quelle dient die Datenverwaltung des Administrationsservers. Die Datei `bases.cab`, die zum Lieferumfang gehört, wird durch den Order `bases` ersetzt. In diesem Ordner werden die Daten der Update-Pakete abgelegt.

Erstellung einer Aufgabe zur Remote-Installation

Für die Remote-Installation von Kaspersky Endpoint Security ist die Aufgabe *Remote-Programminstallation* vorgesehen. Mit der Aufgabe *Remote-Programminstallation* kann das Installationspaket eines Programms auf allen Computern des Unternehmens bereitgestellt werden. Bevor das Installationspaket bereitgestellt wird, können Sie die Antiviren-Datenbanken in diesem Paket aktualisieren und in den Eigenschaften des Installationspakets die verfügbaren Programmkomponenten auswählen.

In der Verwaltungskonsole (MMC) einer Aufgabe zur Remote-Installation erstellen

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie den Punkt **Kaspersky Security Center Administrationsserver** → **Remote-Installation eines Programms** aus.

Schritt 2. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Zusammen mit Kaspersky Endpoint Security wird auch der Administrationsagent installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 3. Erweitert

Wählen Sie ein Installationspaket für den Administrationsagenten aus. Die ausgewählte Version des Administrationsagenten wird zusammen mit Kaspersky Endpoint Security installiert.

Schritt 4. Einstellungen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Wählen Sie die Mittel für die Programminstallation aus:
  - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.
  - **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.
  - **Durch Betriebssystemmittel mithilfe des Administrationsservers**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

- **Verhalten von Geräten, die von anderen Servern verwaltet werden**. Wählen Sie eine Installationsmethode für Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

- **Anwendung nicht installieren, wenn sie schon installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.

Schritt 5. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 6. Auswahl der Geräte, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.

- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 7: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 8. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 9. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, z. B. `Installation von Kaspersky Endpoint Security für Windows 11.6.0`.

Schritt 10. Aufgabenerstellung abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Die Programminstallation wird im unbeaufsichtigten Modus ausgeführt. Nach der Installation wird im Infobereich der Taskleiste des Benutzercomputers das Symbol hinzugefügt. Wenn das Symbol nichts so aussieht, vergewissern Sie sich, dass Sie das Programm aktiviert haben.

Erstellen einer Aufgabe zur Remote-Installation in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Security Center** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Remote-Installation des Programms** aus.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Installation von Kaspersky Endpoint Security für die Geschäftsführung`.
4. Wählen Sie im Block **Geräte, für welche die Aufgabe vorgesehen ist** den Gültigkeitsbereich der Aufgabe aus.

Schritt 2. Computer für die Installation auswählen

Wählen Sie bei diesem Schritt die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe.

Schritt 3. Einstellungen des Installationspaket anpassen

Passen Sie bei diesem Schritt die Einstellungen des Installationspakets an**:**

1. Wählen Sie das Installationspaket für Kaspersky Endpoint Security für Windows (11.6.0) aus.
2. Wählen Sie ein Installationspaket für den Administrationsagenten aus.

   Die ausgewählte Version des Administrationsagenten wird zusammen mit Kaspersky Endpoint Security installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

3. Wählen Sie im Block **Download des Deinstallationstools erzwingen** die Mittel für die Programminstallation aus:

   - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.
   - **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.

- **Durch Betriebssystemmittel mithilfe des Administrationsservers**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

4. Legen Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** fest, wie viele Anfragen für den Download eines Installationspakets maximal an den Administrationsserver gestellt werden dürfen. Durch die Beschränkung der Anfragen lässt sich eine Überlastung des Netzwerks vermeiden.

5. Legen Sie im Feld **Anzahl der Installationsversuche** fest, wie oft versucht werden darf, das Programm zu installieren. Wenn die Installation von Kaspersky Endpoint Security mit einem Fehler beendet wird, startet die Aufgabe die Installation automatisch erneut.

6. Deaktivieren Sie erforderlichenfalls das Kontrollkästchen **Anwendung nicht installieren, wenn sie schon installiert ist**. Dies erlaubt es beispielsweise, eine ältere Version des Programms zu installieren.

7. Deaktivieren Sie erforderlichenfalls das Kontrollkästchen **Zunächst Version des Betriebssystems prüfen**. Dadurch lässt sich verhindern, dass das Programmpaket heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

8. Aktivieren Sie erforderlichenfalls das Kontrollkästchen **Installation des Installationspakets in Gruppenrichtlinien des Active Directory festlegen**. Die Installation von Kaspersky Endpoint Security wird manuell mit den Mitteln des Administrationsagenten oder mit den Mitteln von Active Directory ausgeführt. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

9. Aktivieren Sie erforderlichenfalls das Kontrollkästchen **Benutzer auffordern, laufende Programme zu schließen**. Bei der Installation von Kaspersky Endpoint Security werden die Ressourcen des Computers beansprucht. Vor dem Beginn der Programminstallation schlägt der Installationsassistent dem Benutzer vor, die laufenden Programme zu schließen. Dadurch lassen sich eine Verlangsamung anderer Programme und mögliche Störungen des Computers verhindern.

10. Wählen Sie im Block **Verhalten der Geräte, die von diesem Server verwaltet werden** eine Methode für die Installation von Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 5. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertig**. Die neue Aufgabe wird in der Aufgabenliste angezeigt. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Start**, um die Aufgabe auszuführen. Die Programminstallation wird im unbeaufsichtigten Modus ausgeführt. Nach der Installation wird im Infobereich der Taskleiste des Benutzercomputers das Symbol hinzugefügt. Wenn das Symbol nichts so aussieht, vergewissern Sie sich, dass Sie das Programm aktiviert haben.

Lokale Programminstallation mithilfe des Assistenten

Die Benutzeroberfläche des Installationsassistenten für das Programm besteht aus einer Abfolge von Fenstern, die den einzelnen Installationsschritten entsprechen.

Um mithilfe des Installationsassistenten das Programm zu installieren oder eine ältere Version des Programms zu aktualisieren,

1. Kopieren Sie den Ordner Lieferumfang auf den Benutzercomputer.
2. Führen Sie setup_kes.exe aus.

   Der Setup-Assistent wird gestartet.

Vorbereitung der Installation

Bevor Kaspersky Endpoint Security auf einem Computer installiert oder eine Vorgängerversion des Programms aktualisiert wird, werden folgende Voraussetzungen überprüft:

- Vorhandensein von inkompatibler Software (Eine Liste der inkompatiblen Software befindet sich in der Datei incompatible.txt, die zum Lieferumfang gehört).
- Erfüllung der Hard- und Softwarevoraussetzungen
- Vorhandensein von Rechten für die Programminstallation

Wenn eine der aufgezählten Voraussetzungen nicht erfüllt ist, erscheint eine entsprechende Meldung auf dem Bildschirm.

Erfüllt der Computer die erforderlichen Voraussetzungen, so führt der Installationsassistent eine Suche nach Kaspersky-Programmen durch, deren gleichzeitige Verwendung zu Konflikten führen kann. Werden solche Programme gefunden, so werden Sie aufgefordert, diese manuell zu entfernen.

Wenn sich unter den gefundenen Programmen Vorgängerversionen von Kaspersky Endpoint Security befinden, werden alle Daten, die migriert werden können (z. B. Aktivierungsinformationen und Programmeinstellungen), gespeichert und bei der Installation von Kaspersky Endpoint Security 11.6.0 für Windows verwendet. Die Vorgängerversion des Programms wird automatisch entfernt. Dies bezieht sich auf folgende Programmversionen:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 für Windows (Version 10.2.6.3733)
- Kaspersky Endpoint Security 10 Service Pack 2 für Windows (Version 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 für Windows (Version 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 für Windows (Version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 für Windows (Version 10.3.3.275)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 für Windows (Version 10.3.3.304)
- Kaspersky Endpoint Security für Windows 11.0.0 (Version 11.0.0.6499)
- Kaspersky Endpoint Security für Windows 11.0.1 (Version 11.0.1.90)

- Kaspersky Endpoint Security 11.0.1 für Windows SF1 (Version 11.0.1.90)
- Kaspersky Endpoint Security 11.1.0 für Windows (Version 11.1.0.15919)
- Kaspersky Endpoint Security 11.1.1 für Windows (Version 11.1.1.126)
- Kaspersky Endpoint Security 11.2.0 für Windows (Version 11.1.0.11.2.0.2254)
- Kaspersky Endpoint Security 11.2.0 für Windows CF1 (Version 11.2.0.2254)
- Kaspersky Endpoint Security 11.3.0 für Windows (Version 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 für Windows (Version 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 für Windows (Version 11.5.0.590).

Komponenten von Kaspersky Endpoint Security

Bei der Installation können Sie auswählen, welche Komponenten von Kaspersky Endpoint Security installiert werden sollen. Die Komponente „Schutz vor bedrohlichen Dateien“ ist für die Installation obligatorisch. Sie können die Installation dieser Komponente nicht abwählen.

Standardmäßig sind alle Programmkomponenten für die Installation gewählt. Eine Ausnahme bilden folgende Komponenten:

- Schutz vor modifizierten USB-Geräten.
- Dateien verschlüsseln
- Vollständige Festplattenverschlüsselung.
- Verwaltung von BitLocker.
- Endpoint Agent. *Endpoint Agent* installiert das Programm Kaspersky Endpoint Agent 3.10 zur Interaktion zwischen dem Programm und den Kaspersky-Lösungen für die Erkennung komplexer Bedrohungen (z. B. Kaspersky Sandbox).

Nach der Programminstallation können Sie die Auswahl der Komponenten ändern. Dazu müssen Sie den Installationsassistenten erneut starten und den Vorgang zur Änderung der Komponentenauswahl auswählen.

Erweiterte Einstellungen

Prozess für die Programminstallation schützen. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).

Kompatibilität mit Citrix PVS gewährleisten. Sie können die Unterstützung von Citrix Provisioning Services für die Installation von Kaspersky Endpoint Security auf einer virtuellen Maschine aktivieren.

Pfad des Programms zur Umgebungsvariablen "%PATH%" hinzufügen. Sie können den Installationspfad zur Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

Programm über die Befehlszeile installieren

Die Installation von Kaspersky Endpoint Security aus der Befehlszeile ist in einem der folgenden Modi möglich:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms
- Im unbeaufsichtigten Modus. Nach dem Start der Installation im unbeaufsichtigten Modus ist Ihre Beteiligung am Installationsvorgang nicht mehr erforderlich. Um das Programm im unbeaufsichtigten Modus zu installieren, verwenden Sie die Parameter `/ s` und `/ qn`.

  Bevor Sie das Programm im unbeaufsichtigten Modus installieren, öffnen und lesen Sie bitte den Endbenutzer-Lizenzvertrag und den Text der Datenschutzrichtlinie. Der Endbenutzer-Lizenzvertrag und der Text der Datenschutzrichtlinie gehören zum Lieferumfang von Kaspersky Endpoint Security. Beginnen Sie nur dann mit der Programminstallation, wenn Sie die Bestimmungen und Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen haben, und sie verstehen und akzeptieren, wenn Sie verstehen und damit einverstanden sind, dass Ihre Daten gemäß der Datenschutzrichtlinie verarbeitet und weitergeleitet werden (einschließlich in Drittländer), und wenn Sie die Datenschutzrichtlinie vollständig gelesen haben und sie verstehen. Wenn Sie nicht mit den Bestimmungen und Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, installieren Sie Kaspersky Endpoint Security nicht und verwenden das Programm nicht.

Um das Programm zu installieren oder eine vorhergehende Programmversion zu aktualisieren, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
   [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<Benutzername> /pKLPASSWD=
   <Kennwort> /pKLPASSWDAREA=<Gültigkeitsbereich des Kennworts>] [/pENABLETRACES=1|0
   /pTRACESLEVEL=<Ablaufverfolgungsstufe>] [/s]
   ```

   oder

   ```
   msiexec /i <Name des Programmpakets> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
   [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<Benutzername> KLPASSWD=<Kennwort>
   KLPASSWDAREA=<Gültigkeitsbereich des Kennworts>] [ENABLETRACES=1|0 TRACESLEVEL=
   <Ablaufverfolgungsstufe>] [/qn]
   ```

`EULA=1`	Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen des Lizenzvertrags müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
`PRIVACYPOLICY=1`	Zustimmung zu der Datenschutzrichtlinie. Der Text der Datenschutzrichtlinie gehört zum Lieferumfang von Kaspersky Endpoint Security.

	Die Datenschutzrichtlinie muss akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
`KSN`	Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network (KSN). Ist der Parameter nicht angegeben, so fordert Kaspersky Endpoint Security beim ersten Start des Programms eine Bestätigung der Teilnahme an KSN. Mögliche Werte: • `1` – Zustimmung zur Teilnahme an KSN. • `0` – Ablehnung der Teilnahme an KSN (Standardwert). Das Programmpaket für Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.
`ALLOWREBOOT=1`	Automatischer Neustart des Computers nach der Installation oder Aktualisierung des Programms, falls erforderlich. Wenn dieser Parameter nicht angegeben ist, ist der automatische Neustart des Computers verboten. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.
`SKIPPRODUCTCHECK=1`	Deaktivieren der Überprüfung auf inkompatible Software. Eine Liste der inkompatiblen Software befindet sich in der Datei incompatible.txt, die zum Lieferumfang gehört. Ist dieser Parameter nicht angegeben, so wird beim Fund inkompatibler Software die Installation von Kaspersky Endpoint Security abgebrochen.
`SKIPPRODUCTUNINSTALL=1`	Verbot, gefundene inkompatible Software automatisch zu entfernen. Ist dieser Parameter nicht angegeben, so versucht Kaspersky Endpoint Security inkompatible Software zu entfernen. Das automatische Entfernen inkompatibler Software kann nicht aktiviert werden, wenn Kaspersky Endpoint Security über den msiexec-Installer installiert wird. Verwenden Sie setup_kes.exe, um das automatische Entfernen inkompatibler Software zu aktivieren.
`KLLOGIN`	Festlegen des Benutzernamens für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Komponente Kennwortschutz). Der Benutzername wird zusammen mit den Parametern `KLPASSWD` und `KLPASSWDAREA` festgelegt. Als Standard wird der Benutzername KLAdmin verwendet.
`KLPASSWD`	Festlegen des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Das Kennwort wird zusammen mit den Parametern `KLLOGIN` und `KLPASSWDAREA` festgelegt). Falls Sie ein Kennwort angegeben haben, aber mithilfe des Parameters `KLLOGIN` keinen Benutzernamen festgelegt haben, wird standardmäßig der Benutzername KLAdmin verwendet.

KLPASSWDAREA	Gibt den Gültigkeitsbereich des Kennworts für den Zugriff auf Kaspersky Endpoint Security an. Wenn der Benutzer versucht, eine Aktion aus diesem Bereich auszuführen, fragt Kaspersky Endpoint Security die Anmeldedaten des Benutzers ab (Parameter KLLOGIN und KLPASSWD). Verwenden Sie das Zeichen ";", um mehrere Werte anzugeben. Mögliche Werte: • SET – Änderung der Programmeinstellungen. • EXIT – Beenden des Programms. • DISPROTECT – Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen. • DISPOLICY – Richtlinie für Kaspersky Security Center deaktivieren. • UNINST – Programm vom Computer entfernen. • DISCTRL – Kontrollkomponenten deaktivieren. • REMOVELIC – Schlüssel entfernen. • REPORTS – Berichte anzeigen.
ENABLETRACES	Ablaufverfolgung für das Programm aktivieren oder deaktivieren. Nach dem Start von Kaspersky Endpoint Security speichert das Programm die Ablaufverfolgungsdateien in einem Ordner %ProgramData%\Kaspersky Lab\KES\Traces. Mögliche Werte: • 1 – Die Ablaufverfolgung des Programms ist aktiviert. • 0 – Die Ablaufverfolgung der Programms ist deaktiviert (Standardwert).
TRACESLEVEL	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • 100 (kritisch). Nur Meldungen über fatale Fehler. • 200 (hoch). Meldungen über alle Fehler, einschließlich fatale. • 300 (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • 400 (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • 500 (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über die Nutzung des Programms im normalen Modus (Standardwert). • 600 (niedrig). Alle Meldungen.
AMPPL	Aktivierung oder Deaktivierung des Schutzes für Prozesse von Kaspersky Endpoint Security unter Verwendung der Technologie AM-PPL (Antimalware Protected Process Light). Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website.

	Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019. Mögliche Werte: • `1` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist aktiviert (Standardwert). • `0` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist deaktiviert.
`RESTAPI`	Programmverwaltung über eine REST API. Für die Programmverwaltung über eine REST API muss ein Benutzername angegeben werden (Parameter `RESTAPI_User`). Mögliche Werte: • `1` – Die Verwaltung über eine REST API ist erlaubt. • `0` – Die Verwaltung über eine REST API ist verboten (Standardwert). Für die Programmverwaltung über eine REST API muss die Verwaltung mithilfe von Administrationssystemen erlaubt sein. Legen Sie dazu den Parameter `AdminKitConnector=1` fest. Wenn Sie das Programm über eine REST API verwalten, kann das Programm nicht mithilfe der Kaspersky-Administrationssysteme verwaltet werden.
`RESTAPI_User`	Benutzername des Windows-Domänen-Benutzerkontos für die Programmverwaltung über eine REST API. Die Programmverwaltung über eine REST API ist nur für diesen Benutzer verfügbar. Geben Sie den Benutzernamen im Format `<DOMAIN>\<UserName>` an (z. B. `RESTAPI_User=COMPANY\Administrator`). Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen. Eine Voraussetzung für die Programmverwaltung über eine REST API ist, dass ein Benutzername hinzugefügt wird.
`RESTAPI_Port`	Port für die Programmverwaltung über eine REST API. Als Standard wird Port 6782 verwendet.
`ADMINKITCONNECTOR`	Programmverwaltung mithilfe von Administrationssystemen. Zu den Administrationssystemen zählt beispielsweise Kaspersky Security Center. Sie können Kaspersky-Administrationssysteme oder Lösungen von Drittanbietern verwenden. Kaspersky Endpoint Security bietet eine entsprechende API. Mögliche Werte: • `1` – Die Programmverwaltung mithilfe von Administrationssystemen ist erlaubt (Standardwert). • `0` – Die Programmverwaltung ist nur über die lokale Schnittstelle erlaubt.

Beispiel:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Nach der Installation des Programms Kaspersky Endpoint Security erfolgt die Aktivierung im Rahmen einer Testlizenz, es sei denn, Sie haben in der Datei setup.ini einen Aktivierungscode angegeben. Die Testlizenz ist in der Regel nur für eine kurze Zeit gültig. Nach Ablauf der Testlizenz stellt Kaspersky Endpoint Security die Funktion ein. Um das Programm weiterhin zu nutzen, müssen Sie das Programm mit einer kommerziellen Lizenz aktivieren, entweder mithilfe des Aktivierungs-Assistenten für das Programm oder durch einen speziellen Befehl.

Bei der Installation oder beim Upgrade des Programms im unbeaufsichtigten Modus wird die Verwendung folgender Dateien unterstützt:

- setup.ini – allgemeine Einstellungen für die Programminstallation
- install.cfg – Einstellungen für das Programm Kaspersky Endpoint Security
- setup.reg – Registrierungsschlüssel

  Registrierungsschlüssel aus der Datei setup.reg werden nur dann in die Registrierung eingetragen, wenn in der Datei setup.ini der Wert `setup.reg` für den Parameter `SetupReg` angegeben ist. Die Datei setup.reg wird von den Kaspersky-Experten erstellt. Es wird davon abgeraten, den Inhalt dieser Datei zu ändern.

Um Einstellungen aus den Dateien setup.ini, install.cfg und setup.reg zu übernehmen, legen Sie diese Dateien im Ordner mit dem Programmpaket für Kaspersky Endpoint Security ab. Sie können die Datei setup.reg auch in einem anderen Ordner ablegen. Wenn Sie dies tun, müssen Sie den Pfad zu der Datei im folgenden Programmsinstallationsbefehl angeben: `SETUPREG=<Pfad zur Datei setup.reg>`.

Remote-Installation des Programms mithilfe von System Center Configuration Manager

Die Anleitung ist gültig für die Version System Center Configuration Manager 2012 R2.

Um das Programm ferngesteuert mithilfe von System Center Configuration Manager zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole von Configuration Manager.
2. Wählen Sie im rechten Konsolenbereich im Abschnitt **Anwendungsverwaltung** den Abschnitt **Pakete**.
3. Klicken Sie im oberen Konsolenbereich in der Symbolleiste auf **Paket erstellen**.

   Der *Assistent zum Erstellen von Paketen und Programmen* wird gestartet.
4. Gehen Sie im Assistenten zum Erstellen von Paketen und Programmen wie folgt vor:

   a. Gehen Sie im Abschnitt **Paket** wie folgt vor:

   - Geben Sie im Feld **Name** den Namen des Installationspakets ein.

- Geben Sie im Feld **Quellordner** den Pfad des Ordners an, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.

b. Wählen Sie im Abschnitt **Programmtyp** die Variante **Standardprogramm**.

c. Gehen Sie im Abschnitt **Standardprogramm** wie folgt vor:

- Geben Sie im Feld **Name** den individuellen Namen des Installationspakets ein (z. B. den Programmnamen mit Versionsangabe).
- Geben Sie im Feld **Befehlszeile** die Befehlszeilenparameter für die Installation von Kaspersky Endpoint Security an.
- Geben Sie mithilfe der Schaltfläche **Durchsuchen** den Pfad der ausführbaren Programmdatei an.
- Vergewissern Sie sich, dass in der Dropdown-Liste **Ausführungsmodus** das Element **Mit Administratorrechten starten** gewählt ist.

d. Gehen Sie im Abschnitt **Anforderungen** wie folgt vor:

- Aktivieren Sie das Kontrollkästchen **Anderes Programm zuerst starten**, damit vor der Installation von Kaspersky Endpoint Security ein anderes Programm gestartet wird.

  Wählen Sie das Programm aus der Dropdown-Liste **Programm** oder geben Sie den Pfad der ausführbaren Datei dieses Programms mithilfe der Schaltfläche **Durchsuchen** an.

- Wählen Sie im Abschnitt **Anforderungen an die Plattform** die Variante **Dieses Programm kann nur auf den angegebenen Plattformen gestartet werden**, damit das Programm auf den angegebenen Betriebssystemen installiert wird.

  Aktivieren Sie in der unten angebrachten Liste die Kontrollkästchen für jene Betriebssysteme, in denen Kaspersky Endpoint Security installiert werden soll.

Dieser Schritt ist optional.

e. Überprüfen Sie im Abschnitt **Zusammenfassung** alle angegebenen Werte und klicken Sie auf **Weiter**.

Das erstellte Installationspaket erscheint im Abschnitt **Pakete** in der Liste für verfügbare Installationspakete.

5. Wählen Sie im Kontextmenü des Installationspakets den Punkt **Verteilen**.

   Der *Assistent zur Software-Verteilung* wird gestartet.

6. Gehen Sie im Assistenten zur Software-Verteilung wie folgt vor:

a. Gehen Sie im Abschnitt **Allgemein** wie folgt vor:

- Geben Sie im Feld **Software** den individuellen Namen des Installationspakets an oder wählen Sie mit der Schaltfläche **Durchsuchen** ein Installationspaket aus der Liste.
- Geben Sie im Feld **Sammlung** den Namen der Gruppe für Computer an, auf denen das Programm installiert werden soll, oder wählen Sie diese Sammlung mithilfe der Schaltfläche **Durchsuchen**.

b. Fügen Sie im Abschnitt **Enthält** die Verteilungspunkte (Weitere Informationen finden Sie in der Dokumentation zu System Center Configuration Manager).

c. Legen Sie erforderlichenfalls im Assistenten zur Software-Verteilung die Werte für weitere Einstellungen fest. Diese Einstellungen sind für die Remote-Installation von Kaspersky Endpoint Security optional.

d. Überprüfen Sie im Abschnitt **Zusammenfassung** alle angegebenen Werte und klicken Sie auf **Weiter**.

Nach Abschluss des Assistenten zur Software-Verteilung wird eine Aufgabe zur Remote-Installation von Kaspersky Endpoint Security erstellt.

Beschreibung der Installationseinstellungen in der Datei setup.ini

Die Datei setup.ini wird verwendet, wenn das Programm aus der Befehlszeile oder mithilfe des Gruppenrichtlinienverwaltungs-Editors für Microsoft Windows installiert wird. Um Einstellungen aus der Datei setup.ini zu übernehmen, legen Sie diese Datei im Ordner mit dem Programmpaket für Kaspersky Endpoint Security ab.

DATEI SETUP.INI HERUNTERLADEN

Die Datei setup.ini besteht aus folgenden Abschnitten:

- `[Setup]` - allgemeine Installationsparameter für das Programm.
- `[Components]` - Auswahl der zu installierenden Programmkomponenten. Wird keine Komponente angegeben, werden alle für dieses Betriebssystem verfügbaren Komponenten installiert. Der Schutz vor bedrohlichen Dateien ist eine obligatorische Komponente und wird unabhängig davon auf dem Computer installiert, welche Einstellungen in diesem Block angegeben sind. Auch die Komponente „Managed Detection and Response“ fehlt in diesem Abschnitt. Um diese Komponente zu installieren, müssen Sie Managed Detection and Response in der Kaspersky Security-Verwaltungskonsole aktivieren.
- `[Tasks]` - Auswahl von Aufgaben, welche in die Aufgabenliste von Kaspersky Endpoint Security aufgenommen werden. Wird keine Aufgabe angegeben, werden alle Aufgaben in die Aufgabenliste von Kaspersky Endpoint Security eingetragen.

Anstelle des Wertes `1` können die Werte `yes`, `on`, `enable`, `enabled` verwendet werden.

Anstelle des Werts `0` können die Werte `no`, `off`, `disable` oder `disabled` verwendet werden.

Parameter in der Datei setup.ini

Abschnitt	Einstellung	Beschreibung
`[Setup]`	`InstallDir`	Pfad des Installationsordners für das Programm.
	`ActivationCode`	Aktivierungscode für Kaspersky Endpoint Security.
	`EULA=1`	Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen des Lizenzvertrags müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.

	`PrivacyPolicy=1`	Zustimmung zu der Datenschutzrichtlinie. Der Text der Datenschutzrichtlinie gehört zum Lieferumfang von Kaspersky Endpoint Security. Die Datenschutzrichtlinie muss akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
	`KSN`	Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network (KSN). Ist der Parameter nicht angegeben, so fordert Kaspersky Endpoint Security beim ersten Start des Programms eine Bestätigung der Teilnahme an KSN. Mögliche Werte: • `1` – Zustimmung zur Teilnahme an KSN. • `0` – Ablehnung der Teilnahme an KSN (Standardwert). Das Programmpaket für Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.
	`Login`	Festlegen des Benutzernamens für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Komponente Kennwortschutz). Der Benutzername wird zusammen mit den Parametern `Password` und `PasswordArea` festgelegt. Als Standard wird der Benutzername KLAdmin verwendet.
	`Kennwort`	Festlegen des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Das Kennwort wird zusammen mit den Parametern `Login` und `PasswordArea` festgelegt). Falls Sie ein Kennwort angegeben haben, aber mithilfe des Parameters `Login` keinen Benutzernamen festgelegt haben, wird standardmäßig der Benutzername KLAdmin verwendet.
	`PasswordArea`	Gibt den Gültigkeitsbereich des Kennworts für den Zugriff auf Kaspersky Endpoint Security an. Wenn der Benutzer versucht, eine Aktion aus diesem Bereich auszuführen, fragt Kaspersky Endpoint Security die Anmeldedaten des Benutzers ab (Parameter für `Anmeldedaten` und `Kennwort`). Verwenden Sie das Zeichen "`;`", um mehrere Werte anzugeben. Mögliche Werte: • `SET` – Änderung der Programmeinstellungen. • `EXIT` – Beenden des Programms.

		• `DISPROTECT` – Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen. • `DISPOLICY` – Richtlinie für Kaspersky Security Center deaktivieren. • `UNINST` – Programm vom Computer entfernen. • `DISCTRL` – Kontrollkomponenten deaktivieren. • `REMOVELIC` – Schlüssel entfernen. • `REPORTS` – Berichte anzeigen.
	`SelfProtection`	Schutzmechanismus für die Programminstallation aktivieren oder deaktivieren. Mögliche Werte: • `1` – Das Modul für den Schutz der Programminstallation ist aktiviert (Standardwert). • `0` – Das Modul für den Schutz der Programminstallation ist deaktiviert. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).
	`Reboot=1`	Automatischer Neustart des Computers nach der Installation oder Aktualisierung des Programms, falls erforderlich. Wenn dieser Parameter nicht angegeben ist, ist der automatische Neustart des Computers verboten. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.
	`AddEnvironment`	Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, zur Systemvariablen %PATH% hinzufügen. Mögliche Werte: • `1` – Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird zur Systemvariablen %PATH% hinzugefügt.

		• `0` – Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird nicht zur Systemvariablen %PATH% hinzugefügt.
	`AMPPL`	Aktivierung oder Deaktivierung des Schutzes für Prozesse von Kaspersky Endpoint Security unter Verwendung der Technologie AM-PPL (Antimalware Protected Process Light). Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019. Mögliche Werte: • `1` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist aktiviert (Standardwert). • `0` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist deaktiviert.
	`SetupReg`	Aktivierung der Aufnahme von Registrierungsschlüsseln aus der Datei setup.reg in die Registrierung. Parameterwert `SetupReg: setup.reg`.
	`EnableTraces`	Ablaufverfolgung für das Programm aktivieren oder deaktivieren. Nach dem Start von Kaspersky Endpoint Security speichert das Programm die Ablaufverfolgungsdateien in einem Ordner %ProgramData%\Kaspersky Lab\KES\Traces. Mögliche Werte: • `1` – Die Ablaufverfolgung des Programms ist aktiviert. • `0` – Die Ablaufverfolgung der Programms ist deaktiviert (Standardwert).
	`TracesLevel`	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • `100` (kritisch). Nur Meldungen über fatale Fehler. • `200` (hoch). Meldungen über alle Fehler, einschließlich fatale. • `300` (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • `400` (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • `500` (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über

		die Nutzung des Programms im normalen Modus (Standardwert). • `600` (niedrig). Alle Meldungen.
	`RESTAPI`	Programmverwaltung über eine REST API. Für die Programmverwaltung über eine REST API muss ein Benutzername angegeben werden (Parameter `RESTAPI_User`). Mögliche Werte: • `1` – Die Verwaltung über eine REST API ist erlaubt. • `0` – Die Verwaltung über eine REST API ist verboten (Standardwert). Für die Programmverwaltung über eine REST API muss die Verwaltung mithilfe von Administrationssystemen erlaubt sein. Legen Sie dazu den Parameter `AdminKitConnector=1` fest. Wenn Sie das Programm über eine REST API verwalten, kann das Programm nicht mithilfe der Kaspersky-Administrationssysteme verwaltet werden.
	`RESTAPI_User`	Benutzername des Windows-Domänen-Benutzerkontos für die Programmverwaltung über eine REST API. Die Programmverwaltung über eine REST API ist nur für diesen Benutzer verfügbar. Geben Sie den Benutzernamen im Format `<DOMAIN>\<UserName>` an (z. B. `RESTAPI_User=COMPANY\Administrator`). Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen. Eine Voraussetzung für die Programmverwaltung über eine REST API ist, dass ein Benutzername hinzugefügt wird.
	`RESTAPI_Port`	Port für die Programmverwaltung über eine REST API. Als Standard wird Port 6782 verwendet.
`[Components]`	`ALL`	Installation aller Komponenten. Wenn der Parameterwert `1` angegeben ist, werden alle Komponenten installiert. In diesem Fall bleiben die Parameter, die für die Installation der einzelnen Komponenten angegeben sind, unberücksichtigt.
	`MailThreatProtection`	Schutz vor E-Mail-Bedrohungen.
	`WebThreatProtection`	Schutz vor Web-Bedrohungen.
	`AMSI`	AMSI-Schutz.
	`HostIntrusionPrevention`	Programm-Überwachung.
	`BehaviorDetection`	Verhaltensanalyse.
	`ExploitPrevention`	Exploit-Prävention.
	`RemediationEngine`	Rollback von schädlichen Aktionen
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Schutz vor Netzwerkbedrohungen

	`WebControl`	Web-Kontrolle
	`DeviceControl`	Gerätekontrolle
	`ApplicationControl`	Programmkontrolle.
	`AdaptiveAnomaliesControl`	Adaptive Kontrolle von Anomalien.
	`FileEncryption`	Bibliotheken für die Verschlüsselung von Dateien.
	`DiskEncryption`	Bibliotheken für die vollständige Festplattenverschlüsselung.
	`BadUSBAttackPrevention`	Schutz vor modifizierten USB-Geräten
	`AntiAPT`	Endpoint Agent. *Endpoint Agent* installiert das Programm Kaspersky Endpoint Agent 3.10 zur Interaktion zwischen dem Programm und den Kaspersky-Lösungen für die Erkennung komplexer Bedrohungen (z. B. Kaspersky Sandbox).
	`AdminKitConnector`	Programmverwaltung mithilfe von Administrationssystemen. Zu den Administrationssystemen zählt beispielsweise Kaspersky Security Center. Sie können Kaspersky-Administrationssysteme oder Lösungen von Drittanbietern verwenden. Kaspersky Endpoint Security bietet eine entsprechende API. Mögliche Werte: • `1` – Die Programmverwaltung mithilfe von Administrationssystemen ist erlaubt (Standardwert). • `0` – Die Programmverwaltung ist nur über die lokale Schnittstelle erlaubt.
`[Tasks]`	`ScanMyComputer`	Aufgabe zur vollständigen Untersuchung. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.
	`ScanCritical`	Aufgabe zur Untersuchung wichtiger Bereiche. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.
	`Updater`	Update-Aufgabe. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.

Auswahl der Programmkomponenten ändern

Bei der Programminstallation können Sie die Komponenten auswählen, die verfügbar sein sollen. Sie können die Zusammensetzung des Programms wie folgt ändern:

- Lokal mithilfe des Installationsassistenten für das Programm.

  Die Zusammensetzung des Programms wird mit den üblichen Mitteln des Windows-Betriebssystems geändert, also über die Systemsteuerung. Starten Sie den Installationsassistenten und wählen Sie das Ändern der Auswahl der Programmkomponenten aus. Folgen Sie den Anweisungen auf dem Bildschirm.

- Per Fernzugriff mithilfe von Kaspersky Security Center.

  Um die Auswahl der Komponenten von Kaspersky Endpoint Security nach der Programminstallation zu ändern, können Sie die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Für eine Änderung der Auswahl der Programmkomponenten gelten die folgenden Besonderheiten:

- Auf einem Computer mit dem Betriebssystem Windows Server können nicht alle Komponenten von Kaspersky Endpoint Security installiert werden (z. B. ist die Komponente „Adaptive Kontrolle von Anomalien“ nicht verfügbar).

- Wenn Festplatten auf dem Computer durch die vollständige Festplattenverschlüsselung (FDE) verschlüsselt sind, kann die Komponente „Vollständige Festplattenverschlüsselung“ nicht entfernt werden. Um die Komponente „Vollständige Festplattenverschlüsselung“ zu entfernen, entschlüsseln Sie alle Festplatten des Computers.

- Wenn auf dem Computer verschlüsselte Dateien (FLE) vorhanden sind oder der Benutzer verschlüsselte Wechseldatenträger (FDE oder FLE) verwendet, ist ein Zugriff auf die Daten und Wechseldatenträger nicht mehr möglich, nachdem die Datenverschlüsselungskomponenten entfernt wurden. Sie können Zugriff auf die Daten und Wechseldatenträger erhalten, wenn Sie die Datenverschlüsselungskomponenten neu installieren.

Hinzufügen oder Löschen von Programmkomponenten in der Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie den Punkt **Kaspersky Endpoint Security für Windows (11.6.0) → Auswahl der Programmkomponenten ändern** aus.

Schritt 2. Einstellungen für die Aufgabe zum Ändern der Programmkomponenten

Wählen Sie die Programmkomponenten aus, die auf dem Benutzercomputer verfügbar sein sollen.

Aktivieren Sie das Kontrollkästchen **Inkompatible Programme von Drittherstellern entfernen**. Eine Liste der inkompatiblen Programme ist in der Datei `incompatible.txt` verfügbar, die zum Lieferumfang gehört. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.

Aktivieren Sie erforderlichenfalls den Kennwortschutz für die Aufgabenausführung:

1. Klicken Sie auf **Erweitert**.
2. Aktivieren Sie das Kontrollkästchen **Kennwort für das Ändern der Auswahl der Programmkomponenten verwenden**.
3. Geben Sie die Anmeldedaten des Benutzers KLAdmin ein.

Schritt 3. Auswahl der Geräte, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgaben ein, z. B. `Komponente „Programmkontrolle“ hinzufügen`.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Dadurch wird auf den Benutzercomputern die Auswahl der Komponenten von Kaspersky Endpoint Security im unbeaufsichtigten Modus geändert. Auf der lokalen Programmoberfläche werden die Einstellungen für die verfügbaren Komponenten angezeigt. Programmkomponenten, die nicht ausgewählt wurden, sind deaktiviert und die Einstellungen für diese Komponenten sind nicht verfügbar.

Hinzufügen oder Löschen von Programmkomponenten in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Auswahl der Programmkomponenten ändern** aus.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Komponente „Programmkontrolle“ hinzufügen`.
4. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Sie können beispielsweise eine bestimmte Administrationsgruppe auswählen oder eine Auswahl erstellen.

Schritt 3. Aufgabenerstellung abschließen

Aktivieren Sie das Kontrollkästchen **Nach dem Erstellen das Eigenschaftenfenster der Aufgabe öffnen** und schließen Sie den Assistenten ab. Wählen Sie in den Aufgabeneigenschaften die Registerkarte **Programmeinstellungen** aus und wählen Sie die Programmkomponenten aus, die verfügbar sein sollen.

Aktivieren Sie erforderlichenfalls den Kennwortschutz für die Aufgabenausführung:

1. Aktivieren Sie im Block **Erweiterte Einstellungen** das Kontrollkästchen **Kennwort für das Ändern der Komponentenauswahl verwenden**.
2. Geben Sie die Anmeldedaten des Benutzers KLAdmin ein.

Speichern Sie die vorgenommenen Änderungen und starten Sie die Aufgabe.

Dadurch wird auf den Benutzercomputern die Auswahl der Komponenten von Kaspersky Endpoint Security im unbeaufsichtigten Modus geändert. Auf der lokalen Programmoberfläche werden die Einstellungen für die verfügbaren Komponenten angezeigt. Programmkomponenten, die nicht ausgewählt wurden, sind deaktiviert und die Einstellungen für diese Komponenten sind nicht verfügbar.

Upgrade einer Vorgängerversion des Programms

Das Upgrade einer Vorgängerversion des Programms besitzt die folgenden Besonderheiten:

- Kaspersky Endpoint Security 11.6.0 ist mit Kaspersky Security Center 12 kompatibel.
- Vor Beginn des Programm-Upgrades sollten Sie alle laufenden Programme schließen.
- Wenn im Computer Festplatten vorhanden sind, für welche die vollständige Festplattenverschlüsselung (FDE) verwendet wird, müssen für das Upgrade von Kaspersky Endpoint Security von Version 10 auf Version 11.0.0 und höher alle verschlüsselten Festplatten entschlüsselt werden.

  Vor dem Upgrade blockiert Kaspersky Endpoint Security die Funktionalität zur vollständigen Festplattenverschlüsselung. Falls die Funktionalität zur vollständigen Festplattenverschlüsselung nicht blockiert werden kann, wird die Upgrade-Installation nicht gestartet. Nach dem Programm-Upgrade wird die Funktionalität zur vollständigen Festplattenverschlüsselung wiederhergestellt.

Kaspersky Endpoint Security unterstützt ein Update der folgenden Programmversionen:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 für Windows (Version 10.2.6.3733)
- Kaspersky Endpoint Security 10 Service Pack 2 für Windows (Version 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 für Windows (Version 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 für Windows (Version 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 für Windows (Version 10.3.3.275)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 für Windows (Version 10.3.3.304)
- Kaspersky Endpoint Security für Windows 11.0.0 (Version 11.0.0.6499)
- Kaspersky Endpoint Security für Windows 11.0.1 (Version 11.0.1.90)
- Kaspersky Endpoint Security 11.0.1 für Windows SF1 (Version 11.0.1.90)
- Kaspersky Endpoint Security 11.1.0 für Windows (Version 11.1.0.15919)
- Kaspersky Endpoint Security 11.1.1 für Windows (Version 11.1.1.126)
- Kaspersky Endpoint Security 11.2.0 für Windows (Version 11.1.0.11.2.0.2254)
- Kaspersky Endpoint Security 11.2.0 für Windows CF1 (Version 11.2.0.2254)
- Kaspersky Endpoint Security 11.3.0 für Windows (Version 11.3.0.773)
- Kaspersky Endpoint Security 11.4.0 für Windows (Version 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 für Windows (Version 11.5.0.590).

Bei einem Upgrade von Kaspersky Endpoint Security 10 Service Pack 2 für Windows auf die Version Kaspersky Endpoint Security 11.6.0 für Windows werden die Dateien, die in der älteren Programmversion ins Backup und in die Quarantäne verschoben wurden, in das Backup der neuen Programmversion übertragen. Für Versionen von Kaspersky Endpoint Security, die älter sind als Kaspersky Endpoint Security 10 Service Pack 2 für Windows, werden jene Dateien, die in der älteren Programmversion ins Backup und in die Quarantäne verschoben wurden, nicht übertragen.

Um das Programm Kaspersky Endpoint Security auf einem Computer zu aktualisieren, gibt es folgende Möglichkeiten:

- lokal mithilfe des Installationsassistenten für das Programm.
- lokal aus der Befehlszeile
- per Fernzugriff mithilfe von Kaspersky Security Center 12.
- per Fernzugriff über den Gruppenrichtlinien-Editor von Microsoft Windows (Details finden Sie auf der *Website des Technischen Support von Microsoft*).
- per Fernzugriff mithilfe von System Center Configuration Manager

Ist im Unternehmensnetzwerk das Programm mit einem Komponentensatz verteilt, der sich vom Standardsatz unterscheidet, so unterscheidet sich das Programm-Upgrade über die Verwaltungskonsole (MMC) vom Programm-Upgrade über „Web Console“ und „Cloud Console“. Das Update von Kaspersky Endpoint Security hat die folgenden Besonderheiten:

- Kaspersky Security Center Web Console oder Kaspersky Security Center Cloud Console.

  Wenn Sie ein Installationspaket für die neue Programmversion mit dem standardmäßigen Komponentensatz erstellt haben, wird der Komponentensatz auf dem Benutzercomputer nach dem Upgrade nicht verändert. Um Kaspersky Endpoint Security mit dem standardmäßigen Komponentensatz zu verwenden, gehen Sie wie folgt vor: Öffnen Sie die Eigenschaften des Installationspakets, ändern Sie den Komponentensatz, setzen Sie den Komponentensatz auf den ursprünglichen Zustand zurück und speichern Sie die Änderungen.

- Kaspersky Security Center Verwaltungskonsole.

  Nach dem Upgrade entspricht der Komponentensatz des Programms dem Komponentensatz im Installationspaket. Wenn die neue Programmversion den standardmäßigen Komponentensatz besitzt, wird beispielsweise die Komponente „Schutz vor modifizierten USB-Geräten“ vom Computer gelöscht, da diese Komponente nicht zum Standardsatz gehört. Um das Programm weiterhin mit dem bisherigen Komponentensatz zu verwenden, müssen die erforderlichen Komponenten in den Einstellungen des Installationspakets ausgewählt werden.

Programm löschen

Wenn Kaspersky Endpoint Security entfernt wird, sind der Computer und die Benutzerdaten ungeschützt.

Um das Programm Kaspersky Endpoint Security von einem Computer zu entfernen, gibt es die folgenden Möglichkeiten:

- lokal mithilfe des Installationsassistenten für das Programm.
- lokal aus der Befehlszeile.

- per Fernzugriff mithilfe von Kaspersky Security Center (Details finden Sie in der *Hilfe zu Kaspersky Security Center*)
- per Fernzugriff über den Gruppenrichtlinien-Editor von Microsoft Windows (Details finden Sie auf der *Website des Technischen Support von Microsoft*).

Wenn Sie bei der Installation des Programms die Komponente Endpoint Agent ausgewählt haben, werden die beiden folgenden Programme auf dem Computer installiert: Kaspersky Endpoint Security und Kaspersky Endpoint Agent. Nach der Deinstallation von Kaspersky Endpoint Security wird auch das Programm Kaspersky Endpoint Agent automatisch entfernt.

Deinstallation über Kaspersky Security Center

Sie können das Programm ferngesteuert entfernen mithilfe der Aufgabe *Remote-Deinstallation des Programms*. Wenn diese Aufgabe ausgeführt wird, lädt Kaspersky Endpoint Security ein Hilfsprogramm für die Programm-Deinstallation auf den Benutzercomputer herunter. Nach Abschluss der Programm-Deinstallation wird das Hilfsprogramm automatisch gelöscht.

Entfernen des Programms über die Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie den Punkt **Kaspersky Security Center Administrationsserver → Erweitert → Remote-Deinstallation des Programms** aus.

Schritt 2. Auswahl des zu entfernenden Programms

Wählen Sie **Programm deinstallieren, das von Kaspersky Security Center unterstützt wird** aus.

Schritt 3. Einstellungen für die Aufgabe zum Entfernen des Programms

Wählen Sie den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

Schritt 4. Einstellungen des Deinstallations-Hilfsprogramms

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Deinstallationstools erzwingen**. Wählen Sie aus, auf welche Weise das Hilfsprogramm bereitgestellt werden soll:
  - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten deinstalliert.
  - **Durch Microsoft-Windows-Mittel mithilfe des Administrationsservers**. Das Hilfsprogramm wird durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
  - **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Tool wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.
- **Zunächst Version des Betriebssystems prüfen**. Deaktivieren Sie dieses Kontrollkästchen bei Bedarf. Dadurch lässt sich verhindern, dass das Deinstallations-Hilfsprogramm heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

Wenn der Vorgang zur Programm-Deinstallation durch ein Kennwort geschützt ist, gehen Sie wie folgt vor:

1. Aktivieren Sie das Kontrollkästchen **Deinstallations-Kennwort verwenden**.
2. Klicken Sie auf **Ändern**.
3. Geben Sie das Kennwort des Benutzerkontos KLAdmin ein.

Schritt 5. Einstellungen für den Neustart des Betriebssystems auswählen

Nach der Programm-Deinstallation ist ein Neustart erforderlich. Wählen Sie aus, welche Aktion zum Neustart des Computers ausgeführt werden soll.

Schritt 6. Auswahl der Geräte, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 7: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Es ist nicht erforderlich, für die Deinstallation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten, ein Benutzerkonto auszuwählen.

Schritt 8. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 9. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, z. B. `Deinstallation von Kaspersky Endpoint Security 11.6.0`.

Schritt 10. Aufgabenerstellung abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Die Programm-Deinstallation wird im unbeaufsichtigten Modus ausgeführt.

So entfernen Sie das Programm über die Web Console und die Cloud Console

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Security Center** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Remote-Deinstallation des Programms** aus.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, z. B. `Deinstallation von Kaspersky Endpoint Security auf den Computern des Technischen Supports`.
4. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Sie können beispielsweise eine bestimmte Administrationsgruppe auswählen oder eine Auswahl erstellen.

Schritt 3. Einstellungen für die Programm-Deinstallation anpassen

Passen Sie bei diesem Schritt die Einstellungen für die Programm-Deinstallation an:

1. Wählen Sie den Typ **Verwaltetes Programm entfernen** aus.
2. Wählen Sie den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.
3. **Download des Deinstallationstools erzwingen**. Wählen Sie aus, auf welche Weise das Hilfsprogramm bereitgestellt werden soll:

   - **Mithilfe des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten deinstalliert.
   - **Durch Microsoft-Windows-Mittel mithilfe des Administrationsservers**. Das Hilfsprogramm wird durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
   - **Durch Betriebssystemmittel mithilfe von Verteilungspunkten**. Das Tool wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Details über die Verwendung von Verteilungspunkten *finden Sie in der Hilfe zu Kaspersky Security Center*.

4. Legen Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** fest, wie viele Anfragen für den Download des Hilfsprogramms zur Programm-Deinstallation maximal an den Administrationsserver gestellt werden dürfen. Durch die Beschränkung der Anfragen lässt sich eine Überlastung des Netzwerks vermeiden.

5. Legen Sie im Feld **Anzahl der Deinstallationsversuche** fest, wie oft versucht werden darf, das Programm zu deinstallieren. Wenn die Deinstallation von Kaspersky Endpoint Security mit einem Fehler beendet wird, startet die Aufgabe die Deinstallation automatisch erneut.

6. Deaktivieren Sie erforderlichenfalls das Kontrollkästchen **Zunächst Version des Betriebssystems prüfen**. Dadurch lässt sich verhindern, dass das Deinstallations-Hilfsprogramm heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Es ist nicht erforderlich, für die Deinstallation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten, ein Benutzerkonto auszuwählen.

Schritt 5. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertig**. Die neue Aufgabe wird in der Aufgabenliste angezeigt.

Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Start**, um die Aufgabe auszuführen. Die Programm-Deinstallation wird im unbeaufsichtigten Modus ausgeführt. Nach dem Abschluss der Deinstallation fragt Kaspersky Endpoint Security, ob der Computer neu gestartet werden soll.

Falls der Vorgang zur Programm-Deinstallation kennwortgeschützt ist, geben Sie in den Eigenschaften der Aufgabe *Remote-Deinstallation des Programms* das Kennwort des Benutzerkontos KLAdmin ein. Ohne Kennwort wird die Aufgabe nicht ausgeführt.

Um in der Aufgabe „Remote-Deinstallation des Programms" das Kennwort des Benutzerkontos KLAdmin zu verwenden, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console" den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die folgende Aufgabe von Kaspersky Security Center: **Remote-Deinstallation des Programms**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Aktivieren Sie das Kontrollkästchen **Deinstallations-Kennwort verwenden**.

5. Geben Sie das Kennwort des Benutzerkontos KLAdmin ein.

6. Klicken Sie auf **Speichern**.

Deinstallation des Programms mithilfe des Assistenten

Kaspersky Endpoint Security wird mit den gewöhnlichen Mitteln des Windows-Betriebssystems entfernt: über die Systemsteuerung. Der Setup-Assistent wird gestartet. Folgen Sie den Anweisungen auf dem Bildschirm.

Hier können Sie festlegen, welche vom Programm verwendeten Daten Sie beibehalten möchten, um sie später bei einer Neuinstallation des Programms (z. B. Installation einer neueren Version) wiederzuverwenden. Wenn Sie keine Daten angeben, wird das Programm vollständig entfernt.

Sie können folgende Daten speichern:

- **Aktivierungsdaten** sind Daten, die es erlauben, das Programm künftig nicht erneut zu aktivieren. Kaspersky Endpoint Security fügt automatisch einen Lizenzschlüssel hinzu, falls die Lizenz zum Zeitpunkt der Installation nicht abgelaufen ist.
- **Backup-Dateien** sind Dateien, die vom Programm untersucht und ins Backup verschoben wurden.

  Der Zugriff auf Backup-Dateien, die nach der Deinstallation des Programms gespeichert bleiben, ist nur mit der Programmversion möglich, in welcher die Dateien gespeichert wurden.

  Falls Sie Backup-Objekte nach der Programm-Deinstallation verwenden möchten, müssen Sie diese vor der Deinstallation des Programms wiederherstellen. Die Kaspersky-Experten raten jedoch davon ab, Objekte aus dem Backup wiederherzustellen, da dadurch der Computer beschädigt werden kann.

- **Programmeinstellungen** sind Einstellungen für die Programmausführung, die im Verlauf der Programmnutzung angepasst wurden.
- Der **lokale Speicher für Chiffrierschlüssel** enthält Daten, die den Zugriff auf jene Dateien und Datenträger ermöglichen, die vor der Programm-Deinstallation verschlüsselt wurden. Um auf verschlüsselte Dateien und Datenträger zuzugreifen, vergewissern Sie sich, dass Sie bei der erneuten Installation von Kaspersky Endpoint Security die Funktionalität zur Datenverschlüsselung ausgewählt haben. Für den Zugriff auf früher verschlüsselte Dateien und Datenträger sind keine weiteren Maßnahmen erforderlich.

Programm über die Befehlszeile deinstallieren

Für die Deinstallation von Kaspersky Endpoint Security aus der Befehlszeile gibt es die folgenden Modi:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms
- Im unbeaufsichtigten Modus. Nach dem Start der Deinstallation im unbeaufsichtigten Modus ist Ihre Beteiligung am Deinstallationsvorgang nicht mehr erforderlich. Um das Programm im unbeaufsichtigten Modus zu entfernen, verwenden Sie die Parameter `/ s` und `/ qn`.

Um das Programm im unbeaufsichtigten Modus zu entfernen, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.

3. Führen Sie den folgenden Befehl aus:

- Wenn der Deinstallationsvorgang nicht kennwortgeschützt ist:

  ```
  setup_kes.exe /s /x
  ```

  oder

  ```
  msiexec.exe /x <GUID> /qn
  ```

  wobei `<GUID>` – einmalige Programm-ID. Die Programm-GUID können Sie mithilfe des folgenden Befehls ermitteln:

  ```
  wmic product where „Name like '%Kaspersky Endpoint Security%'“ get Name, IdentifyingNumber
  ```

- Wenn der Deinstallationsvorgang kennwortgeschützt ist:

  ```
  setup_kes.exe /pKLLOGIN=<Benutzername> /pKLPASSWD=<Kennwort> /s /x
  ```

  oder

  ```
  msiexec.exe /x <GUID> KLLOGIN=<Benutzername> KLPASSWD=<Kennwort> /qn
  ```

Beispiel:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

Lizenzverwaltung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

Über den Endbenutzer-Lizenzvertrag

Der *Lizenzvertrag* ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig durch, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Lizenzbedingungen können Sie wie folgt einsehen:

- Im interaktiven Modus während der Installation von Kaspersky Endpoint Security.
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms und befindet sich auch im Installationsordner des Programms `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\<Gebietsschema>\KES`.

Wenn Sie bei der Programminstallation den Lizenzbedingungen zustimmen, gilt Ihr Einverständnis mit den Lizenzbedingungen als erteilt. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird.

Die Lizenz berechtigt Sie zur Nutzung folgender Leistungen:

- Nutzung des Programm in Übereinstimmung mit den Bedingungen des Lizenzvertrags
- Nutzung des Technischen Supports

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer für das Programm sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Testlizenz* - kostenlose Lizenz zum Kennenlernen des Programms.

  Die Testlizenz ist in der Regel nur für eine kurze Zeit gültig. Nach Ablauf der Testlizenz stellt Kaspersky Endpoint Security die Funktion ein. Um das Programm weiterhin nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Sie können das Programm nur ein Mal mit der Testlizenz aktivieren.

- *Kommerzielle Lizenz* - kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

Die im Rahmen einer kommerziellen Lizenz verfügbare Programmfunktionalität ist von der Auswahl des Produkts abhängig. Das ausgewählte Produkt ist im Lizenzzertifikat angegeben. Informationen über die verfügbaren Produkte finden Sie auf der Website von Kaspersky.

Wenn die kommerzielle Lizenz abläuft, werden wichtige Funktionen der App deaktiviert. Um die App weiterhin nutzen zu können, müssen Sie Ihre kommerzielle Lizenz verlängern. Wenn Sie Ihre Lizenz nicht verlängern möchten, müssen Sie die App von Ihrem Computer entfernen.

Über das Lizenzzertifikat

Das *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit der Schlüsseldatei oder dem Aktivierungscode erhalten.

Das Lizenzzertifikat enthält folgende Informationen über die vorliegende Lizenz:

- Lizenzschlüssel oder Bestellnummer
- Informationen über den Benutzer, für den die Lizenz ausgestellt wurde
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- quantitative Beschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf)
- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über das Abo

Ein Abonnement für Kaspersky Endpoint Security ist ein Auftrag, nach dem das Programm mit bestimmten Einstellungen (Abo-Laufzeit, Anzahl der geschützten Geräte) genutzt werden kann. Ein Abo für Kaspersky Endpoint Security kann bei einem Provider registriert werden (z. B. bei einem Internet-Provider). Das Abo kann manuell oder automatisch verlängert oder auch gekündigt werden. Das Abonnement kann auf der Webseite des Dienstanbieters verwaltet werden.

Es gibt beschränkte (z. B. auf ein Jahr) und unbefristete (ohne Ablaufdatum) Abos. Um Kaspersky Endpoint Security weiterhin zu nutzen, müssen Sie ein beschränktes Abonnement rechtzeitig verlängern. Ein unbefristetes Abo wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Provider überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abo-Verlängerung gewährt, während der die Programmfunktionalität erhalten bleibt. Das Angebot und die Dauer einer Nachfrist sind vom Dienstanbieter abhängig.

Um Kaspersky Endpoint Security im Rahmen eines Abonnements zu nutzen, müssen Sie den Aktivierungscode anwenden, den Sie vom Dienstanbieter erhalten haben. Nachdem der Aktivierungscode angewendet wurde, wird der aktive Schlüssel hinzugefügt. Der aktive Schlüssel bestimmt die Lizenz für die Verwendung des Programms im Rahmen des Abonnements. Im Rahmen eines Abonnements kann kein Reserveschlüssel hinzugefügt werden.

Auf Grundlage eines Abos erworbene Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Endpoint Security genutzt werden.

Über den Lizenzschlüssel

Ein *Lizenzschlüssel* ist eine Bitsequenz, mit der Sie das Programm in Übereinstimmung mit den Bedingungen des Endbenutzer-Lizenzvertrags aktivieren und anschließend verwenden können.

Für Schlüssel, die im Rahmen eines Abonnements hinzugefügt werden, gibt es kein Lizenzzertifikat.

Einen Lizenzschlüssel können Sie wie folgt zum Programm hinzufügen: Schlüsseldatei anwenden oder Aktivierungscode eingeben.

Kaspersky kann einen Schlüssel blockieren, wenn die Bedingungen des Lizenzvertrags verletzt werden. Wenn ein Schlüssel gesperrt ist, müssen Sie einen anderen Schlüssel hinzufügen, damit das Programm funktioniert.

Ein Schlüssel kann entweder ein aktiver Schlüssel oder ein Reserveschlüssel sein.

Ein *aktiver Schlüssel* ist ein Schlüssel, der momentan für das Programm verwendet wird. Als aktiver Schlüssel kann entweder ein Schlüssel für eine Testlizenz oder für eine kommerzielle Lizenz hinzugefügt werden. Im Programm kann es nur einen aktiven Schlüssel geben.

Ein *Reserveschlüssel* gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet. Nach Ablauf des aktiven Schlüssels wird automatisch der Reserveschlüssel aktiviert. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Ein Schlüssel für eine Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Er kann nicht als Reserveschlüssel hinzugefügt werden. Ein aktiver Schlüssel kann nicht durch einen Schlüssel für eine Testlizenz ersetzt werden.

Wenn ein Schlüssel zur Liste der verbotenen Schlüssel hinzugefügt wird, bleibt der Funktionsumfang des Programms, der durch die zur Aktivierung des Programms verwendete Lizenz definiert ist, acht Tage lang verfügbar. Das Programm benachrichtigt den Benutzer, dass der Schlüssel zur Liste der verbotenen Schlüssel hinzugefügt wurde. Nach Ablauf von acht Tagen entspricht die Programmfunktionalität jener Situation, in der die Lizenz abgelaufen ist. Sie können die Schutz- und Kontrollkomponenten verwenden und eine Untersuchung ausführen. Dabei werden die Programm-Datenbanken verwendet, die bei Ablauf der Lizenz installiert waren. Außerdem verschlüsselt das Programm weiterhin Dateien, die geändert werden und vor Ablauf der Lizenz verschlüsselt worden sind. Neue Dateien werden aber nicht mehr verschlüsselt. Kaspersky Security Network kann nicht genutzt werden.

Über den Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Sequenz aus zwanzig lateinischen Buchstaben und Ziffern. Wenn Sie den Aktivierungscode eingeben, wird ein Lizenzschlüssel hinzugefügt, der Kaspersky Endpoint Security aktiviert. Der Aktivierungscode wird an Ihre angegebene E-Mail-Adresse gesendet, nachdem Sie Kaspersky Endpoint Security gekauft haben.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, ist für den Zugriff auf die Kaspersky-Aktivierungsserver eine Internetverbindung erforderlich.

Wenn das Programm mithilfe eines Aktivierungscodes aktiviert wird, wird ein aktiver Schlüssel hinzugefügt. Ein Reserveschlüssel kann nur mithilfe eines Aktivierungscodes hinzugefügt werden und nicht mithilfe einer Schlüsseldatei.

Wenn ein Aktivierungscode nach der Programmaktivierung verloren geht, können Sie den Aktivierungscode wiederherstellen. Der Aktivierungscode kann beispielsweise für die Registrierung bei Kaspersky CompanyAccount erforderlich sein. Falls Sie den Aktivierungscode nach der Programmaktivierung verlieren, wenden Sie sich an den Kaspersky-Partner, bei dem Sie die Lizenz gekauft haben.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Ihnen von Kaspersky bereitgestellt wird. Mit der Schlüsseldatei wird ein Lizenzschlüssel für die Programmaktivierung hinzugefügt.

Die Schlüsseldatei wird an Ihre angegebene E-Mail-Adresse gesendet, nachdem Sie Kaspersky Endpoint Security gekauft oder nachdem Sie die Testversion von Kaspersky Endpoint Security bestellt haben.

Um das Programm mithilfe einer Schlüsseldatei zu aktivieren, ist kein Zugriff auf die Kaspersky-Aktivierungsserver erforderlich.

Wenn eine Schlüsseldatei versehentlich gelöscht wurde, können Sie die Datei wiederherstellen. Eine Schlüsseldatei kann beispielsweise für die Registrierung bei Kaspersky CompanyAccount erforderlich sein.

Es bestehen folgende Möglichkeiten, um eine Schlüsseldatei wiederherzustellen:

- Kontaktaufnahme mit dem Verkäufer.
- Auf der Kaspersky-Website mithilfe des vorhandenen Aktivierungscodes eine Schlüsseldatei anfordern.

Wenn das Programm mithilfe einer Schlüsseldatei aktiviert wird, wird ein aktiver Schlüssel hinzugefügt. Ein Reserveschlüssel kann nur mithilfe einer Schlüsseldatei hinzugefügt werden und nicht mithilfe eines Aktivierungscodes.

Programm aktivieren

Durch die *Aktivierung* erlangt die Lizenz, die zur Nutzung der Premiumversion des Programms berechtigt, ihre Gültigkeit für den entsprechenden Zeitraum. Beim Aktivierungsvorgang des Programms wird ein Lizenzschlüssel hinzugefügt.

Sie können das Programm auf eine der folgenden Weisen aktivieren:

- Lokal von der Programmoberfläche aus können Sie mithilfe des Aktivierungsassistenten sowohl den aktiven Schlüssel als auch den Reserveschlüssel auf diese Weise hinzufügen.
- Ferngesteuert mithilfe des Programmpakets Kaspersky Security Center. Dazu wird eine Aufgabe zum Hinzufügen eines Lizenzschlüssels erstellt und anschließend gestartet. Auf diese Weise können Sie einen aktiven Schlüssel und einen Reserveschlüssel hinzufügen.
- Ferngesteuerte Verteilung von Lizenzdateien und Aktivierungscodes, die sich in der Schlüsselablage auf dem Kaspersky Security Center Administrationsserver befinden, an die Client-Computer. Details über die Verteilung von Schlüsseln *finden Sie in der Hilfe zu Kaspersky Security Center*. Auf diese Weise können Sie einen aktiven Schlüssel und einen Reserveschlüssel hinzufügen.

Ein Aktivierungscode, der mit einem Abo erworben wurde, wird zuerst verteilt.

- Mithilfe der Befehlszeile.

Wenn das Programm ferngesteuert oder bei der Programminstallation im Silent-Modus mit einem Aktivierungscode aktiviert wird, kann es aufgrund der Auslastung der Kaspersky-Aktivierungsserver zu Verzögerungen kommen. Sollte eine sofortige Programmaktivierung notwendig sein, so können Sie die laufende Aktivierung abbrechen und das Programm mithilfe des Aktivierungs-Assistenten aktivieren.

Aktivierung des Programms über Kaspersky Security Center

Es gibt folgende Möglichkeiten, um das Programm ferngesteuert über Kaspersky Security Center zu aktivieren:

- Mithilfe der Aufgabe *Schlüssel hinzufügen*.

  Auf diese Weise kann der Schlüssel auf einem konkreten Computer oder auf den Computern, die zu einer Administrationsgruppe gehören, hinzugefügt werden.

- Durch die Verteilung eines Schlüssels, der sich auf dem Administrationsserver für Kaspersky Security Center befindet, an die Computer.

  Mit dieser Methode kann ein Schlüssel automatisch auf bereits mit Kaspersky Security Center verbundenen Computern und auf neuen Computern hinzugefügt werden. Um diese Methode zu verwenden, müssen Sie zuerst einen Schlüssel zum Kaspersky Security Center Administrationsserver hinzufügen. Details über das Hinzufügen von Schlüsseln zum Administrationsserver für Kaspersky Security Center *finden Sie in der Hilfe für Kaspersky Security Center*.

Für Kaspersky Security Center Cloud Console ist eine Testversion vorgesehen. Die *Testversion* ist eine spezielle Version von Kaspersky Security Center Cloud Console. Sie dient dazu, die Funktionen von Kaspersky Security Center Cloud Console kennenzulernen. In dieser Version können Sie einen Arbeitsbereich für einen Zeitraum von 30 Tagen verwenden. Im Rahmen der Testlizenz für Kaspersky Security Center Cloud Console werden alle verwalteten Programme automatisch ausgeführt, einschließlich Kaspersky Endpoint Security. Nachdem die Testlizenz für Kaspersky Security Center Cloud Console abläuft, kann Kaspersky Endpoint Security nicht im Rahmen einer eigenen Testlizenz aktiviert werden. Details über die Lizenzverwaltung von Kaspersky Security Center *finden Sie in der Hilfe für Kaspersky Security Center Cloud Console*.

Die Testversion von Kaspersky Security Center Cloud Console erlaubt es nicht, anschließend zur kommerziellen Version zu wechseln. Ein beliebiger Test-Arbeitsbereich wird mit seinem gesamten Inhalt nach Ablauf von 30 Tagen gelöscht.

Es gibt folgende Möglichkeiten, um die Verwendung von Lizenzen zu kontrollieren:

- *Bericht über die Schlüsselnutzung* in der Unternehmensinfrastruktur anzeigen (**Monitoring und Berichte** → **Berichte**).

- Status der Computer auf der Registerkarte **Geräte** → **Verwaltete Geräte** anzeigen. Wenn das Programm nicht aktiviert ist, hat der Computer den Status ⚠ und die Statusbeschreibung **Das Programm ist nicht aktiviert**.

- Informationen über die Lizenz in den Computereigenschaften anzeigen.

- Schlüsseleigenschaften anzeigen (**Vorgänge** → **Lizenzverwaltung**).

[Aktivieren des Programms in der Verwaltungskonsole (MMC)]

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (11.6.0) → Schlüssel hinzufügen**.

Schritt 2. Schlüssel hinzufügen

Geben Sie einen Aktivierungscode ein oder wählen Sie eine Schlüsseldatei aus.

Details über das Hinzufügen von Schlüsseln zur Datenverwaltung von Kaspersky Security Center *finden Sie in der Hilfe zu Kaspersky Security Center*.

Schritt 3. Auswahl der Geräte, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, beispielsweise `Aktivierung von Kaspersky Endpoint Security für Windows`.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch wird auf den Benutzercomputern das Programm Kaspersky Endpoint Security im unbeaufsichtigten Modus aktiviert.

Aktivieren des Programms in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Schlüssel hinzufügen** aus.

3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Aktivierung von Kaspersky Endpoint Security für Windows`.

4. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus. Klicken Sie auf **Weiter**.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.

- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Lizenz auswählen

Wählen Sie eine Lizenz aus, mit der Sie das Programm aktivieren möchten. Klicken Sie auf **Weiter**.

Sie können Schlüssel in der „Web Console“ hinzufügen (**Vorgänge** → **Lizenzverwaltung**).

Schritt 4. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertig**. Die neue Aufgabe wird in der Aufgabenliste angezeigt. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Start**, um die Aufgabe auszuführen. Dadurch wird auf den Benutzercomputern das Programm Kaspersky Endpoint Security im unbeaufsichtigten Modus aktiviert.

In den Eigenschaften der Aufgabe *Schlüssel hinzufügen* können Sie auf dem Computer einen Reserveschlüssel hinzufügen. Der *Reserveschlüssel* wird aktiviert, wenn der aktive Schlüssel abläuft oder wenn der aktive Schlüssel gelöscht wird. Mit einem Reserveschlüssel lässt sich verhindern, dass die Programmfunktionalität beim Ablauf der Lizenz beschränkt wird.

Automatisches Hinzufügen eines Lizenzschlüssels für Computer über die Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Lizenzen für Kaspersky-Software**.

   Die Liste der Lizenzschlüssel wird geöffnet.

2. Öffnen Sie die Eigenschaften des Lizenzschlüssels.

3. Aktivieren Sie im Abschnitt **Allgemein** das Kontrollkästchen **Automatisch zu verteilender Lizenzschlüssel**.

4. Speichern Sie die vorgenommenen Änderungen.

   Dadurch wird der Schlüssel automatisch an die passenden Computer verteilt. Wenn ein Schlüssel automatisch als aktiver Schlüssel oder als Reserveschlüssel verteilt wird, wird die Lizenzbeschränkung für die Anzahl der Computer berücksichtigt. Diese Beschränkung ist in den Schlüsseleigenschaften angegeben. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels an die Computer automatisch beendet. Die Anzahl der Computer, auf denen der Schlüssel hinzugefügt wurde, sowie andere Daten können in den Schlüsseleigenschaften im Abschnitt **Geräte** eingesehen werden.

Automatisches Hinzufügen eines Lizenzschlüssels über „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Vorgänge** → **Lizenzverwaltung** → **Lizenzen für Kaspersky-Software** aus.

   Die Liste der Lizenzschlüssel wird geöffnet.

2. Öffnen Sie die Eigenschaften des Lizenzschlüssels.

3. Schalten Sie auf der Registerkarte **Allgemein** den Schalter **Schlüssel automatisch verteilen** ein.

4. Speichern Sie die vorgenommenen Änderungen.

   Dadurch wird der Schlüssel automatisch an die passenden Computer verteilt. Wenn ein Schlüssel automatisch als aktiver Schlüssel oder als Reserveschlüssel verteilt wird, wird die Lizenzbeschränkung für die Anzahl der Computer berücksichtigt. Diese Beschränkung ist in den Schlüsseleigenschaften angegeben. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels an die Computer automatisch beendet. Die Anzahl der Computer, auf denen der Schlüssel hinzugefügt wurde, sowie andere Daten können in den Schlüsseleigenschaften auf der Registerkarte **Geräte** eingesehen werden.

Programm mithilfe des Aktivierungsassistenten aktivieren

Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security mithilfe des Aktivierungsassistenten zu aktivieren:

1. Klicken Sie auf die Schaltfläche **Lizenz**, die sich im unteren Bereich des Programmhauptfensters befindet.

2. Klicken Sie im geöffneten Fenster auf die Schaltfläche **Das Programm mit einer neuen Lizenz aktivieren**.

Der Aktivierungsassistent für das Programm wird gestartet. Folgen Sie den Anweisungen des Aktivierungsassistenten.

Programm über die Befehlszeile aktivieren

Um das Programm mithilfe der Befehlszeile zu aktivieren,

geben Sie in der Befehlszeile Folgendes ein:

```
avp.com license /add <Aktivierungscode oder Schlüsseldatei> [/login=<Benutzername>
/password=<Kennwort>]
```

Die Anmeldedaten des Benutzers (`/login=<Benutzername> /password=<Kennwort>`) müssen eingegeben werden, wenn der Kennwortschutz aktiviert ist.

Lizenz-Info anzeigen

Um Informationen über die Lizenz anzuzeigen,

Klicken Sie auf die Schaltfläche **Lizenz** am unteren Rand des Programmhauptfensters.

Das Fenster **Lizenzverwaltung** wird geöffnet. Dieses Fenster zeigt Informationen über die Lizenz an (siehe Abbildung unten).

Fenster Lizenzverwaltung

Das Fenster **Lizenzverwaltung** enthält folgende Informationen:

- **Status des Schlüssels**. Auf dem Computer können mehrere Schlüssel vorhanden sein. Ein Schlüssel kann entweder ein aktiver Schlüssel oder ein Reserveschlüssel sein. Im Programm kann es nur einen aktiven Schlüssel geben. Ein Reserveschlüssel kann erst zum aktiven Schlüssel werden, nachdem der aktive Schlüssel abläuft oder nachdem der aktive Schlüssel mithilfe der Schaltfläche gelöscht wurde.

- **Schlüssel**. Ein *Schlüssel* ist eine einmalige alphanumerische Zeichenfolge, die auf dem Aktivierungscode und der Schlüsseldatei basiert.

- **Lizenzen**. Es sind folgende Lizenztypen vorgesehen: Test und kommerziell.

- **Programmname**. Vollständiger Name des erworbenen Kaspersky-Programm.

- **Funktionalität**. Programmfunktionen, die im Rahmen Ihrer Lizenz verfügbar sind. Es sind die folgenden Funktionen vorgesehen: Schutz, Sicherheitskontrolle, Datenverschlüsselung und andere. Eine Liste der verfügbaren Funktionen ist auch im Lizenzzertifikat verfügbar.

- **Zusatzinformationen über die Lizenz**. Lizenztyp, Anzahl der Computer, auf die sich die Lizenz erstreckt, Anfangsdatum und Ende (Datum und Uhrzeit) der Gültigkeitsdauer der Lizenz (nur für den aktiven Schlüssel).

  Die Uhrzeit für den Ablauf der Gültigkeitsdauer der Lizenz wird in der Zeitzone angezeigt, die im Betriebssystem festgelegt ist.

Im Fenster der Lizenzverwaltung sind außerdem die folgenden Aktionen verfügbar:

- **Lizenz kaufen** / **Lizenz verlängern**. Öffnet die Website des Online-Shops von Kaspersky. Dort können Sie eine Lizenz kaufen oder die Gültigkeitsdauer der Lizenz verlängern. Dazu müssen Sie die Daten Ihres Unternehmens eingeben und den Auftrag bezahlen.

- **Programm mit neuer Lizenz aktivieren** Startet den Aktivierungsassistenten für das Programm. Der Assistent ermöglicht es, einen Schlüssel mithilfe des Aktivierungscodes oder der Schlüsseldatei hinzuzufügen. Mithilfe des Assistenten zur Programmaktivierung können ein aktiver Schlüssel und ein einziger Reserveschlüssel hinzugefügt werden.

Lizenz kaufen

Sie können die Lizenz auch nach der Installation des Programms erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode oder eine Schlüsseldatei, um das Programm zu aktivieren.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche **Lizenz**.

2. Führen Sie im Fenster **Lizenzverwaltung** eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Lizenz kaufen**, wenn kein einziger Schlüssel hinzugefügt wurde oder nur der Schlüssel einer Testlizenz vorhanden ist.

   - Klicken Sie auf die Schaltfläche **Lizenz verlängern**, wenn ein Schlüssel für die kommerzielle Lizenz hinzugefügt wurde.

   Die Website des Kaspersky-Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Abo verlängern

Wenn das Programm im Abo genutzt wird, greift Kaspersky Endpoint Security bis zum Ablauf des Abos in bestimmten Zeitabständen automatisch auf den Aktivierungsserver zu.

Wenn Sie das Programm mit einem unbefristeten Abo nutzen, überprüft Kaspersky Endpoint Security im Hintergrundmodus automatisch, ob auf dem Aktivierungsserver ein aktualisierter Schlüssel vorliegt. Wenn auf dem Aktivierungsserver ein Schlüssel liegt, ersetzt das Programm den vorherigen Schlüssel durch den neuen. Ein unbefristetes Abo für Kaspersky Endpoint Security wird ohne Ihr Eingreifen verlängert.

Wenn Sie das Programm im Rahmen eines befristeten Abonnements nutzen, werden Sie an dem Tag, an dem das Abonnement oder die Nachfrist für die Abo-Verlängerung nach dem Ablauf des Abonnements endet, von Kaspersky Endpoint Security darüber informiert und die Versuche zur automatischen Abo-Verlängerung werden eingestellt. Hierbei verhält sich Kaspersky Endpoint Security genau so wie nach dem Ablauf einer kommerziellen Lizenz für die Programmnutzung, d. h. das Programm funktioniert weiterhin, wird aber nicht mehr aktualisiert und kann nicht auf Kaspersky Security Network zugreifen.

Sie können das Abonnement auf der Website des Dienstanbieters verlängern.

Sie können den Abo-Status im Fenster **Lizenzverwaltung** manuell aktualisieren. Dies kann erforderlich sein, wenn das Abonnement nach Ablauf der Nachfrist verlängert wurde und das Programm den Abo-Status nicht automatisch aktualisiert.

Um von der Programmoberfläche aus auf die Provider-Webseite zu gelangen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche **Lizenz**.

2. Klicken Sie im Fenster **Lizenzverwaltung** auf **Abo-Provider kontaktieren**.

Bereitstellung von Daten im Rahmen des Endbenutzer-Lizenzvertrags

Wenn für die Aktivierung von Kaspersky Endpoint Security ein Aktivierungscode verwendet wird, stimmen Sie zu, dass automatisch die folgenden Informationen regelmäßig an Kaspersky übertragen werden, damit die Rechtmäßigkeit der Programmverwendung überprüft werden kann:

- Typ, Version und Sprachversion von Kaspersky Endpoint Security
- Versionen der installierten Updates für Kaspersky Endpoint Security
- ID des Computers und ID der Installation von Kaspersky Endpoint Security auf dem Computer
- Seriennummer und ID des aktiven Schlüssels
- Typ, Version und Bit-Version des Betriebssystems, Name der virtuellen Umgebung, falls das Programm Kaspersky Endpoint Security in einer virtuellen Umgebung installiert ist
- IDs der Komponenten von Kaspersky Endpoint Security, die zum Zeitpunkt der Datenbereitstellung aktiv sind.

Kaspersky kann diese Informationen auch verwenden, um statistische Informationen über die Verbreitung und Verwendung von Kaspersky-Software zu erstellen.

Wenn Sie einen Aktivierungscode verwenden, stimmen Sie der automatischen Übertragung der oben genannten Daten zu. Wenn Sie es ablehnen, Kaspersky diese Informationen bereitzustellen, muss für die Aktivierung von Kaspersky Endpoint Security eine Schlüsseldatei verwendet werden.

Wenn Sie die Bedingungen des Lizenzvertrags akzeptieren, stimmen Sie der automatischen Weitergabe folgender Informationen zu:

- Beim Update von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - ID von Kaspersky Endpoint Security
  - aktiver Schlüssel;
  - einmalige ID für den Start der Update-Aufgabe
  - einmalige ID der Installation von Kaspersky Endpoint Security.
- Beim Wechsel mithilfe von Links aus der Benutzeroberfläche von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - Version des Betriebssystems
  - Aktivierungsdatum von Kaspersky Endpoint Security
  - Ablaufdatum der Lizenz

- Erstellungsdatum des Schlüssels
- Installationsdatum von Kaspersky Endpoint Security
- ID von Kaspersky Endpoint Security
- ID der gefundenen Schwachstelle des Betriebssystems
- ID des zuletzt installierten Updates für Kaspersky Endpoint Security
- Hash der gefundenen Datei, die eine Bedrohung darstellt, und Bezeichnung dieses Objekts nach der Kaspersky-Klassifikation
- Kategorie des Aktivierungsfehlers für Kaspersky Endpoint Security
- Code des Aktivierungsfehlers für Kaspersky Endpoint Security
- Anzahl der Tage bis zum Ablauf des Schlüssels
- Anzahl der Tage, die seit dem Hinzufügen des Schlüssels vergangen sind
- Anzahl der Tage, die seit dem Ablauf der Lizenz vergangen sind
- Anzahl der Computer, auf die sich die aktuelle Lizenz erstreckt
- aktiver Schlüssel;
- Gültigkeitsdauer der Lizenz für Kaspersky Endpoint Security
- aktueller Status der Lizenz
- Typ der aktuellen Lizenz
- Typ des Programms
- einmalige ID für den Start der Update-Aufgabe
- einmalige ID der Installation von Kaspersky Endpoint Security auf dem Computer
- Sprache der Benutzeroberfläche von Kaspersky Endpoint Security

Kaspersky schützt die erhaltenen Informationen in Übereinstimmung mit geltenden gesetzlichen Bestimmungen und mit den aktuellen Richtlinien von Kaspersky. Die Daten werden über verschlüsselte Verbindungskanäle übertragen.

Ausführliche Angaben darüber, wie Informationen über die Programmverwendung empfangen, verarbeitet, gespeichert und gelöscht werden, nachdem der Lizenzvertrag und die Erklärung zu Kaspersky Security Network akzeptiert worden sind, finden Sie in den genannten Dokumenten und auf der Kaspersky-Website. Die Dateien license.txt und ksn_<ID der Sprache>.txt mit den Texten des Endbenutzer-Lizenzvertrags und der Erklärung zu Kaspersky Security Network gehören zum Lieferumfang des Programms.

Datenbereitstellung bei der Verwendung von Kaspersky Security Network

Der Datensatz, den Kaspersky Endpoint Security an Kaspersky sendet, hängt von der Art der Lizenz und den Nutzungseinstellungen des Kaspersky Security Network ab.

Verwendung von KSN unter Lizenz auf nicht mehr als 4 Computern

Wenn Sie die Erklärung zu Kaspersky Security Network akzeptieren, stimmen Sie der automatischen Übertragung folgender Informationen zu:

- Informationen über das Update der KSN-Konfiguration: ID der aktuellen Konfiguration, ID der erhaltenen Konfiguration, Fehlercode des Konfigurations-Updates.
- Informationen über untersuchte Dateien und Webadressen: Prüfsummen der untersuchten Datei (MD5, SHA2-256, SHA1) und der Dateimuster (MD5), Größe des Musters, Typ der gefundenen Bedrohung und Bedrohungsname gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken, Webadresse, für welche die Reputation abgefragt wird, sowie Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde, ID des Verbindungsprotokolls und Nummer des verwendeten Ports;
- ID der Untersuchungsaufgabe, die die Bedrohung entdeckt hat;
- Informationen über verwendete digitale Zertifikate, welche für ihre Authentifizierung erforderlich sind: Prüfsummen (SHA256) des Zertifikats, mit welchem das Untersuchungsobjekt signiert ist, und des öffentlichen Zertifikatschlüssels;
- ID der Software-Komponente, welche die Untersuchung ausführt.
- ID der Antiviren-Datenbanken und der Einträge in den Antiviren-Datenbanken.
- Informationen über die Aktivierung der Software auf dem Computer: signierter Header des Tickets vom Aktivierungsdienst (ID des regionalen Aktivierungszentrums, Prüfsumme des Aktivierungscodes, Prüfsumme des Tickets, Erstellungsdatum des Tickets, Ticketversion, Lizenzstatus, Datum und Uhrzeit für den Beginn und den Ablauf der Ticketgültigkeit, einmalige Lizenz-ID, Lizenzversion), ID des Zertifikats, mit dem der Ticket-Header signiert ist, Prüfsumme (MD5) der Schlüsseldatei;
- Informationen über den Rechteinhaber der Software: Typ und vollständige Programmversion von Kaspersky Endpoint Security, Version des verwendeten Protokolls für die Verbindung mit den Kaspersky-Diensten.

Nutzung von KSN unter Lizenz auf 5 oder mehr Computern

Wenn Sie die Erklärung zu Kaspersky Security Network akzeptieren, stimmen Sie der automatischen Übertragung folgender Informationen zu:

Ist das Kontrollkästchen **Kaspersky Security Network** aktiviert und das Kontrollkästchen **Erweiterten KSN-Modus aktivieren** deaktiviert, so werden die folgenden Informationen übertragen:

- Informationen über das Update der KSN-Konfiguration: ID der aktuellen Konfiguration, ID der erhaltenen Konfiguration, Fehlercode des Konfigurations-Updates.
- Informationen über untersuchte Dateien und Webadressen: Prüfsummen der untersuchten Datei (MD5, SHA2-256, SHA1) und der Dateimuster (MD5), Größe des Musters, Typ der gefundenen Bedrohung und Bedrohungsname gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken, Webadresse, für welche die Reputation abgefragt wird, sowie Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde, ID des Verbindungsprotokolls und Nummer des verwendeten Ports;
- ID der Untersuchungsaufgabe, die die Bedrohung entdeckt hat;
- Informationen über verwendete digitale Zertifikate, welche für ihre Authentifizierung erforderlich sind: Prüfsummen (SHA256) des Zertifikats, mit welchem das Untersuchungsobjekt signiert ist, und des öffentlichen Zertifikatschlüssels;

- ID der Software-Komponente, welche die Untersuchung ausführt.

- ID der Antiviren-Datenbanken und der Einträge in den Antiviren-Datenbanken.

- Informationen über die Aktivierung der Software auf dem Computer: signierter Header des Tickets vom Aktivierungsdienst (ID des regionalen Aktivierungszentrums, Prüfsumme des Aktivierungscodes, Prüfsumme des Tickets, Erstellungsdatum des Tickets, Ticketversion, Lizenzstatus, Datum und Uhrzeit für den Beginn und den Ablauf der Ticketgültigkeit, einmalige Lizenz-ID, Lizenzversion), ID des Zertifikats, mit dem der Ticket-Header signiert ist, Prüfsumme (MD5) der Schlüsseldatei;

- Informationen über den Rechteinhaber der Software: Typ und vollständige Programmversion von Kaspersky Endpoint Security, Version des verwendeten Protokolls für die Verbindung mit den Kaspersky-Diensten.

Sind die Kontrollkästchen **Kaspersky Security Network** und **Erweiterten KSN-Modus aktivieren** aktiviert, so werden zusätzlich zu den oben genannten Informationen auch die folgenden Informationen übertragen:

- Informationen zu den Ergebnissen der Kategorisierung der angeforderten Webressourcen, welche folgende Angaben enthält: untersuchte Webadresse und IP-Adresse des Hosts, Version der Software-Komponente, welche die Kategorisierung ausgeführt hat, Kategorisierungsmethode und Auswahl der Kategorien, welche für diese Webressource ermittelt wurden;

- Informationen über die auf dem Computer installierte Software: Name der Softwareanwendungen und Softwareanbieter, Registrierungsschlüssel und ihre Werte, Informationen über Dateien der installierten Softwarekomponenten (Prüfnummern (MD5, SHA2-256, SHA1), Name, Dateipfad auf dem Computer, Größe, Version und die digitale Signatur).

- Informationen über den Stand des Virenschutzes des Computers: die Versionen und die Versions-Zeitstempel der verwendeten Antiviren-Datenbanken, die ID der Aufgabe und die ID der Software, die die Untersuchung durchführt;

- Informationen über die Dateien, die vom Benutzer heruntergeladen wurden: Webadressen und IP-Adressen, von welchen der Download erfolgt ist, und Webadresse der Seite, von welcher auf die Seite für den Datei-Download gewechselt wurde, ID des Download-Protokolls und Nummer des Verbindungsports, Merkmal für die Schädlichkeit von Adressen; Attribute, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei; Informationen zum Prozess, welcher die Datei heruntergeladen hat (Prüfsummen (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung, Merkmal für das Vorhandensein im Autostart, Attribute, Namen von Packprogrammen, Informationen zur Signatur, Merkmal der ausführbaren Datei, Format-ID, Typ des Benutzerkontos, von welchem der Prozess gestartet wurde), Informationen zur Prozessdatei (Name, Pfad und Größe der Datei), Dateiname, Dateipfad auf dem Computer, digitale Signatur der Datei und Informationen über die Signierung, Webadresse, bei welcher der Fund erfolgte, Nummer des Skripts auf der Webseite, die als verdächtig oder schädlich eingestuft wurde;

- Informationen über gestartete Programme und deren Module: Daten über gestartete Prozesse im System (Prozess-ID im System (PID), Prozessname, Daten über das Benutzerkonto, von dem der Prozess gestartet wurde, Programm und Befehl, welcher den Prozess gestartet hat, Merkmal für die Vertrauenswürdigkeit des Programms oder des Prozesses, vollständiger Pfad der Prozessdateien und Prüfsummen (MD5, SHA2-256, SHA1), Befehlszeile für den Start, Integritätsniveau des Prozesses, Beschreibung des Produkts, zu welchem der Prozess gehört (Name des Produkts und Daten zum Herausgeber), sowie Daten über verwendete digitale Zertifikate und Informationen, die für ihre Authentifizierung erforderlich sind, oder Daten über das Fehlen einer digitalen Signatur für die Datei), sowie Informationen über die Module, welche in Prozesse geladen wurden (Name, Größe, Typ, Erstellungsdatum, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfad), Informationen zur Kopfzeile für PE-Dateien, Name des Packprogramms (falls die Datei gepackt ist);

- Informationen über alle potentiell schädlichen Objekte und Aktionen: Name des erkannten Objekts und vollständiger Pfad des Objekts auf dem Computer, Prüfsummen der verarbeiteten Objekte (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) des Fundes; Namen, Größe und Pfade der verarbeiteten Dateien; Code der Pfadvorlage, Merkmal der ausführbaren Datei, Merkmal, ob das Objekt ein Container ist, Name des Packprogramms (falls die Datei gepackt war), Code des Dateityps, ID des Dateiformats, ID der Antiviren-

Datenbanken und der Einträge in den Antiviren-Datenbanken, auf deren Basis die Entscheidung der Software getroffen wurde, Merkmal des potentiell schädlichen Objekts, Name der gefundenen Bedrohung gemäß der Klassifikation des Rechteinhabers, Gefährlichkeitsstufe, Status und Erkennungsmethode, Grund der Aufnahme in den analysierten Kontext und Ordnungsnummer der Datei im Kontext, Prüfsummen (MD5, SHA2-256, SHA1), Name und Attribute der ausführbaren Datei der Anwendung, über welche die infizierte Nachricht oder der Link eingedrungen ist, IP-Adressen (IPv4 und IPv6) des Hosts des blockierten Objekts, Datei-Entropie, Merkmal für das Vorhandensein der Datei im Autostart, Zeitpunkt (Datum und Uhrzeit) des ersten Fundes der Datei im System, Anzahl der Dateistarts seit dem letzten Senden einer Statistik, Compiler-Typ; Informationen über den Namen, die Prüfsummen (MD5, SHA2-256, SHA1) und die Größe des Mail-Clients, über welchen das schädliche Objekt empfangen wurde; ID der Software-Aufgabe, welche die Untersuchung ausgeführt hat; Merkmal für die Überprüfung der Reputation oder der Signatur der Datei, Ergebnisse der statistischen Analyse des Objektinhalts, Muster des Objekts, Größe des Musters (in Bytes), technische Eigenschaften der eingesetzten Erkennungstechnologien.

- Informationen über untersuchte Objekte: zugewiesene Sicherheitsgruppe, in welche und/oder aus welcher die Datei verschoben wurde, Grund, aus welchem die Datei in diese Kategorie verschoben wurde, ID der Kategorie, Informationen über die Quelle der Kategorien und Version der Datenbank der Kategorien, Merkmal für das Vorhandensein eines vertrauenswürdigen Zertifikats der Datei, Name des Dateiherstellers, Dateiversion, Name und Version des Programms, zu welcher die Datei gehört;

- Informationen über gefundene Schwachstellen: ID der Schwachstelle in der Datenbank für Schwachstellen, Gefahrenklasse der Schwachstelle.

- Informationen über die Ausführung einer Emulation der ausführbaren Datei: Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Version der Emulationskomponente, Emulationstiefe, Vektor der Merkmale für logische Blöcke und Funktionen innerhalb logischer Blöcke, welche im Verlauf der Emulation erhalten wurden, Daten aus der Struktur der PE-Kopfzeile der ausführbaren Datei;

- IP-Adressen des angreifenden Computers (IPv4 und IPv6), Portnummer auf dem Computer, auf welchen der Netzwerkangriff gerichtet war, ID des Protokolls des IP-Pakets, das den Angriff enthielt, Angriffsziel (Name des Unternehmens, Website), Flag für die Reaktion auf den Angriff, Gewichtung des Angriffs, Vertrauensebene;

- Informationen über Angriffe, welche mit dem Spoofing von Netzwerkressourcen verbunden waren, DNS- und IP-Adressen (IPv4 oder IPv6) der besuchten Websites.

- DNS- und IP-Adressen (IPv4 oder IPv6) der angefragten Web-Ressource, Informationen über die Datei und den Web-Client, der auf die Web-Ressource zugreift, Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1) der Datei, vollständiger Pfad der Datei und der Vorlagencode des Dateipfads, das Ergebnis der Überprüfung der digitalen Signatur und deren Status im KSN.

- Informationen über die Ausführung eines Rollbacks der Aktionen von Schadsoftware: Daten über die Datei, deren Aktivität rückgängig gemacht wurde (Name, vollständiger Pfad, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei), Daten über erfolgreiche und erfolglose Aktionen zur Löschung, Umbenennung und zum Kopieren von Dateien und zur Wiederherstellung von Registrierungswerten (Namen und Werte der Registrierungsschlüssel), Informationen über Systemdateien, welche von der Schadsoftware verändert wurden, vor und nach der Ausführung des Rollbacks.

- Informationen über die Ausnahmen, die für adaptive Abweichkontrollkomponente festgelegt sind: die ID und der Status der Regel, die ausgelöst wurde, die von der Software ausgeführte Aktion, wenn die Regel ausgelöst wurde, der Typ des Benutzerkontos, unter welchem der Prozess oder Thread verdächtige Aktivitäten durchführt, sowie über den Prozess, der Gegenstand von verdächtigen Aktivitäten war (Skript-ID oder Name der Prozessdatei, vollständiger Pfad zur Prozessdatei, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) der Prozessdatei); Informationen über das Objekt, das die verdächtigen Aktionen ausgeführt hat sowie über das Objekt, das Gegenstand von verdächtigen Aktionen war (Name des Registrierschlüssels oder Dateiname, vollständiger Pfad zur Datei, Vorlagencode des Dateipfads und die Prüfsummen (MD5, SHA2-256, SHA1) der Datei).

- Informationen über geladene Software-Module: Name, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Moduldatei, vollständiger Pfad und Code der Pfadvorlage für die Datei, Parameter der digitalen Signatur der

Moduldatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung der Signatur, Name des Subjekts und Organisation, welche die Moduldatei signiert hat, ID des Prozesses, in welchen das Modul geladen wurde, Name des Modulherstellers, Ordnungsnummer des Moduls in der Ladeabfolge.

- Informationen über die Qualität der Softwareinteraktion mit den KSN-Diensten: Datum und Uhrzeit von Beginn und Ende der Periode, in der die Statistiken erzeugt wurden, Informationen über die Qualität der Anfragen und der Verbindung zu den einzelnen verwendeten KSN-Diensten (KSN-Dienstkennung, Anzahl der erfolgreichen Anfragen, Anzahl der Anfragen mit Antworten vom Cache, Anzahl nicht erfolgreicher Anfragen (Netzwerkprobleme, KSN wurde in den Softwareeinstellungen deaktiviert, fehlerhaftes Routing), verbrauchte Zeit der erfolgreichen Anfragen, verbrauchte Zeit der abgebrochenen Anfragen, verbrauchte Zeit der Anfragen mit überschrittener Zeit, Anzahl der Verbindungen zum KSN aus dem Cache, Anzahl der erfolgreichen Verbindungen zum KSN, Anzahl der nicht erfolgreichen Verbindungen zum KSN, Anzahl der erfolgreichen Transaktionen, Anzahl der nicht erfolgreichen Transaktionen, verbrauchte Zeit der erfolgreichen Verbindungen zum KSN, verbrauchte Zeit der nicht erfolgreichen Verbindungen zum KSN, verbrauchte Zeit der erfolgreichen Transaktionen, verbrauchte Zeit der nicht erfolgreichen Transaktionen).

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt: Elemente der Objekthierarchie des Systems (ObjectManager), Daten im UEFI-BIOS-Speicher sowie Namen von Registrierschlüsseln und deren Werte;

- Informationen über Ereignisse in Systemprotokollen: Ereigniszeitpunkt, Name des Protokolls, in welchem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name und Beschreibung der Ereignisquelle;

- Informationen über Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Prozessdatei, des geöffneten Ports, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adresse, Nummern des lokalen und des Remote-Verbindungsports, Verbindungszustand, Dauer, für welche der Port geöffnet war;

- Informationen über das Datum der Softwareinstallation und -aktivierung auf dem Computer: die ID des Partners, der die Lizenz verkauft hat, die Seriennummer der Lizenz, der signierte Header des Tickets vom Aktivierungsdienst (die ID eines regionalen Aktivierungszentrums, die Prüfsumme des Aktivierungscodes, die Prüfsumme des Tickets, das Erstellungsdatum des Tickets, die eindeutige ID des Tickets, die Ticketversion, der Lizenzstatus, das Datum und die Uhrzeit des Ticketbeginns und -endes, die eindeutige ID der Lizenz, die Lizenzversion), die ID des Zertifikats, das zum Signieren des Ticketheaders verwendet wurde, die Prüfsumme (MD5) der Schlüsseldatei, die eindeutige ID der Softwareinstallation auf dem Computer, der Typ und die ID des Programms, die aktualisiert wird, die ID der Update-Aufgabe;

- Informationen über die Zusammensetzung aller installierten Updates sowie über die Zusammensetzung der zuletzt installierten und/oder gelöschten Updates, Typ des Ereignisses, aufgrund dessen Informationen über Updates gesendet wurden, Zeitraum, welcher seit der Installation des letzten Updates vergangen ist, Informationen über die Antiviren-Datenbanken, die zum Zeitpunkt der Datenbereitstellung geladen waren.

- Informationen über die Verwendung der Software auf dem Computer: Daten über die Prozessornutzung (CPU), Daten über die Nutzung des Arbeitsspeichers (Private Bytes, Non-Paged Pool, Paged Pool), Anzahl der aktiven Ströme im Software-Prozess und der Ströme im Wartezustand, Arbeitsdauer der Software bis zum Auftreten des Fehlers, Merkmal für die Verwendung der Software im interaktiven Modus.

- Anzahl der Software-Dumps und der System-Dumps (BSOD) ab dem Zeitpunkt der Software-Installation und ab dem Zeitpunkt des letzten Updates, ID und Version des Software-Moduls, in welchem die Störung aufgetreten ist, Speicherstapel im Produktprozess und Informationen über die Antiviren-Datenbanken zum Zeitpunkt der Störung;

- Daten zum System-Dump (BSOD): Merkmal für das Auftreten des BSOD auf dem Computer, Name des Treibers, welcher den BSOD hervorgerufen hat, Adresse und Speicherstapel im Treiber, Merkmal für die Dauer der Sitzung des Betriebssystems bis zum Auftreten des BSOD, Speicherstapel des Treiberabsturzes, Typ des gespeicherten Arbeitsspeicher-Dumps, Merkmal für die Tatsache, dass die Sitzung des Betriebssystems bis zum BSOD länger als 10 Minuten gedauert hat, einmalige Dump-ID, Zeitpunkt (Datum und Uhrzeit), zu welchem der BSOD aufgetreten ist.

- Informationen über Fehler oder Leistungsprobleme, die bei der Ausführung von Softwarekomponenten aufgetreten sind: Status-ID der Software, Typ, Code und Zeitpunkt des auftretenden Fehlers, IDs der Komponente, des Moduls und des Produktprozesses, in welchem der Fehler aufgetreten ist, ID der Aufgabe oder der Update-Kategorie, in welcher der Fehler aufgetreten ist, Protokolle der von der Software verwendeten Treiber (Fehlercode, Modulname, Name der Quelldatei und Zeile, in welcher der Fehler aufgetreten ist).

- Informationen über die Updates der Antiviren-Datenbanken und der Software-Komponenten: Name, Datum und Uhrzeit der Indexdateien, die beim letzten Update heruntergeladen wurden und beim laufenden Update heruntergeladen werden;

- Informationen über die Abstürze der Software: Erstellungszeitpunkt (Datum und Uhrzeit) und Typ des Dumps, Typ des Ereignisses, welches den Absturz der Software verursacht hat (unerwarteter Stromausfall, Absturz einer Dritthersteller-Anwendung), Zeitpunkt (Datum und Uhrzeit) des unerwarteten Stromausfalls.

- Informationen über die Kompatibilität der Treiber der Software mit der Hard- und Software: Informationen über die Betriebssystemeigenschaften, welche die Funktionalität der Softwarekomponenten beschränken (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), Typ der integrierten Boot-Software (UEFI, BIOS), Merkmal für das Vorhandensein eines Trusted Platform Module (TPM), Version der TPM-Spezifikation, Informationen über den auf dem Computer installierten Hauptprozessor (CPU), Modus und Einstellungen für Code Integrity und Device Guard, Modus der Treiber und Verwendungsgrund für den aktuellen Modus, Version der Treiber der Software, Status der Unterstützung von Treibern für die Soft- und Hardware-Virtualisierung des Computers.

- Informationen über Drittanbieterprogramm, welche einen Fehler verursacht haben: Name, Version und Sprachversion, Fehlercode und Informationen über den Fehler aus dem Systemprotokoll der Programme, Adresse und Speicherstapel für das Auftreten des Fehlers einer Drittanbieterprogramm, Merkmal für das Auftreten des Fehlers in einer Software-Komponente, Arbeitsdauer der Drittanbieterprogramm bis zum Auftreten des Fehlers, Prüfsummen (MD5, SHA2-256, SHA1) des Prozessmusters des Programms, in welcher der Fehler aufgetreten ist, Pfad dieses Prozessmusters des Programms und Code der Pfadvorlage, Informationen aus dem Systemprotokoll des Betriebssystems mit einer Beschreibung des Fehlers, welcher mit dem Programm verbunden war, Informationen über das Programm-Modul, in welchem der Fehler aufgetreten ist (Fehler-ID, Fehleradresse als Offset im Modul, Name und Version des Moduls, ID für den Absturz des Programms in einem Plug-in des Rechteinhabers und Speicherstapel für diesen Absturz, Arbeitsdauer des Programms bis zum Absturz);

- Version der Update-Komponente der Software, Anzahl der Abstürze der Update-Komponente der Software bei der Ausführung von Update-Aufgaben im Rahmen der Komponentenausführung, ID des Typs der Update-Aufgabe, Anzahl der Fehler bei den Update-Aufgaben der Update-Komponente der Software.

- Informationen über die Ausführung von Überwachungskomponenten des Softwaresystems: vollständige Versionen der Komponenten, Datum und Uhrzeit, wann die Komponenten gestartet wurden, Code des Ereignisses, das zum Überlaufen der Warteschlange für Ereignisse geführt hat, und Anzahl solcher Ereignisse, Gesamtzahl der Warteschlangenüberlaufe, Informationen über die Datei des Prozesses, der das Ereignis ausgelöst hat (Name und Pfad der Datei auf dem Computer, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) des mit der Datei verbundenen Prozesses, Dateiversion), ID des Abfangvorgangs, vollständige Version des Abfangfilters, ID für den Typ des abgefangenen Ereignisses, Größe der Ereigniswarteschlange, und Anzahl der Ereignisse zwischen dem ersten Ereignis in der Warteschlange und dem aktuellen Ereignis, Anzahl überfälliger Ereignisse in der Warteschlange, Informationen über die Datei des Prozesses, der das aktuelle Ereignis ausgelöst hat (Name und Pfad der Datei auf dem Computer, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) des mit der Datei verbundenen Prozesses), Dauer der Ereignisverarbeitung, Höchstdauer der Ereignisverarbeitung, Wahrscheinlichkeit für das Senden von Statistiken, Informationen über Ereignisse des Betriebssystems, für die die Verarbeitungszeit überschritten wurde (Datum und Uhrzeit des Ereignisses, Anzahl der wiederholten Initialisierungen der Antiviren-Datenbanken, Datum und Uhrzeit der letzten, wiederholten Initialisierung der Antiviren-Datenbanken nach ihrem Update, Verzögerungszeit der Verarbeitung eines Ereignisses für jede Systemüberwachungskomponente, Anzahl der Ereignisse in der Warteschlange, Anzahl der verarbeiteten Ereignisse, Anzahl der verzögerten Ereignisse des aktuellen Typs, Gesamtverzögerungszeit der Ereignisse des aktuellen Typs, Gesamtverzögerungszeit aller Ereignisse).

- Informationen von dem Windows-Tool zur Ereignisprotokollierung (Event Tracing for Windows, ETW) bei Problemen mit der Leistung der Software, Ereignisanbieter SysConfig / SysConfigEx / WinSATAssessment von Microsoft: Daten über den Computer (Modell, Hersteller, Formfaktor des Gehäuses, Version), Daten über die Windows-Leistungsindikatoren (WinSAT-Bewertungsdaten, Windows-Leistungsindex), Name der Domäne, Daten über die physischen und logischen Prozessoren (Anzahl der physischen und logischen Prozessoren, Hersteller, Modell, Stepping, Anzahl der Kerne, Taktfrequenz, Prozessor-ID (CPUID), Cache-Eigenschaften, Eigenschaften des logischen Prozessors, Merkmale für die Unterstützung der Modi und Anweisungen), Daten über die Module des Arbeitsspeichers (Typ, Formfaktor, Hersteller, Modell, Größe, Granularität der Speicherbelegung), Daten über Netzwerkschnittstellen (IP- und MAC-Adressen, Name, Beschreibung, Konfiguration der Netzwerkschnittstellen, Verteilung der Anzahl und der Größe von Netzwerkpaketen nach Typen, Geschwindigkeit des Netzwerkaustauschs, Verteilung der Anzahl der Netzwerkfehler nach Typen), Konfiguration des IDE-Controllers, IP-Adresse der DNS-Server, Daten über die Grafikkarte (Modell, Beschreibung, Hersteller, Kompatibilität, Größe des Grafikspeichers, Bildschirmauflösung, Anzahl der Bits pro Pixel, BIOS-Version), Daten über verbundene Plug-and-Play-Geräte(Name, Beschreibung, Geräte-ID [PnP, ACPI], Daten über Laufwerke und Speichergeräte (Anzahl der Laufwerke oder Flash-Laufwerke, Hersteller, Modell, Größe des Laufwerks, Anzahl der Zylinder, Anzahl der Spuren pro Zylinder, Anzahl der Sektoren pro Spur, Größe des Sektors, Cache-Eigenschaften, Ordnungszahl, Partitionsanzahl, Konfiguration des SCSI-Controllers), Daten über die logischen Laufwerke (Ordnungszahl, Größe der Partition, Volume-Größe, Volume-Buchstabe, Typ der Partition, Typ des Dateisystems, Anzahl der Cluster, Cluster-Größe, Anzahl der Sektoren pro Cluster, Anzahl der belegten und freien Cluster, Boot-Volume-Buchstabe, Adresse-Abweichung der Partition bezüglich des Anfangs des Laufwerks), Daten über das BIOS der Hauptplatine (Hersteller, Veröffentlichungsdatum, Version), Daten über die Hauptplatine (Hersteller, Modell, Typ), Daten über den physischen Speicher (gesamter und freier Platz), Daten über die Dienste des Betriebssystems (Name, Beschreibung, Status, Tag, Daten über Prozesse [Name und PID-ID]), Energieoptionen des Computers, Konfiguration des Interrupt Controllers, Pfade der Windows-Systemordner (Windows und System32), Daten über das Betriebssystem (Version, Build, Veröffentlichungsdatum, Name, Typ, Installationsdatum), Größe der Auslagerungsdatei, Daten über die Monitore (Anzahl, Hersteller, Bildschirmauflösung, Auflösungsvermögen, Typ), Daten über den Treiber der Grafikkarte (Hersteller, Veröffentlichungsdatum, Version).

- Informationen von ETW, Bereitstellung von EventTrace/EventMetadata Ereignissen von Microsoft: Informationen über die Sequenz von Systemereignissen (Typ, Uhrzeit, Datum, Zeitzone), Metadaten über die Datei mit Trace-Ergebnissen (Name, Struktur, Trace-Parameter, Aufgliederung der Anzahl von Trace-Operationen nach Typ), Informationen über das Betriebssystem (Name, Typ, Version, Build, Veröffentlichungsdatum, Startzeit).

- Informationen von ETW, Bereitstellung von Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power Ereignisse von Microsoft: Informationen über gestartete und abgeschlossene Prozesse (Name, PID, Startparameter, Befehlszeile, Rückgabecode, Energieverwaltungsparameter, Start- und Fertigstellungszeit, Typ des Zugriffstoken, SID, SessionID, Anzahl der installierten Deskriptoren), Informationen über Änderungen der Thread-Prioritäten (TID, Priorität, Uhrzeit), Informationen über Laufwerkoperationen des Prozesses (Typ, Uhrzeit, Kapazität, Anzahl), Verlauf der Änderungen der Struktur und Kapazität der nutzbaren Speicherprozesse.

- Informationen von ETW, Bereitstellung von StackWalk/Perfinfo Ereignissen von Microsoft: Informationen über Leistungsindikatoren (Leistung von einzelnen Codeabschnitten, Sequenz von Funktionsaufrufen, PID, TID, Adressen und Attribute von ISRs und DPCs).

- Informationen von ETW, Bereitstellung von KernelTraceControl-ImageID Ereignissen von Microsoft: Informationen über ausführbare Dateien und dynamische Bibliotheken (Name, Bildgröße, vollständiger Pfad), Informationen zu PDB-Dateien (Name, ID), VERSIONINFO Ressourcendaten für ausführbare Dateien (Name, Beschreibung, Ersteller, Ort, Programmversion und -ID, Dateiversion und -ID);

- Informationen von ETW, Bereitstellung von FileIo/DiskIo/Image/Windows Kernel Disk Ereignissen von Windows: Informationen zu Datei- und Laufwerkoperationen (Typ, Kapazität, Startzeit, Fertigstellungszeit, Dauer, Status der Fertigstellung, PID, TID, Funktionsaufrufadressen des Treibers, E/A-Anfragepaket (IRP), Windows-Dateiobjektattribute), Informationen über Dateien, die in Datei- und Laufwerkoperationen involviert sind (Name, Version, Größe, vollständiger Pfad, Attribute, Offset, Prüfsumme des Bildes, Optionen für das Öffnen und Zugreifen).

- Informationen von ETW, Bereitstellung von PageFault Ereignissen von Microsoft: Informationen über Zugriffsfehler der Speicherseiten (Adresse, Uhrzeit, Kapazität, PID, TID, Attribute von Windows-Dateiobjekten, Parameter der Speicherzuordnung).

- Informationen von ETW, Bereitstellung von Thread Ereignissen von Microsoft: Informationen über Thread-Erstellung/-Fertigstellung, Informationen gestartete Threads (PID, TID, Größe des Stacks, Prioritäten und Zuordnungen von CPU-Ressourcen, E/A-Ressourcen, Speicherseiten zwischen Threads, Stack-Adresse, Adresse der Initialisierungsfunktion, Adresse des Thread Environment Block (TEB), Windows Service-Tag).

- Informationen von ETW, Bereitstellung von Microsoft Windows Kernel Memory Ereignissen von Microsoft: Informationen über Speicherverwaltungsoperationen (Status der Fertigstellung, Uhrzeit, Anzahl, PID), Struktur der Speicherzuordnung (Typ, Kapazität, SessionID, PID).

- Informationen zu Softwareoperationen im Falle von Leistungsproblemen: ID der Softwareinstallation, Typ und Wert des Leistungsabfalls, Informationen über die Sequenz von Ereignissen innerhalb der Software (Uhrzeit, Zeitzone, Typ, Status der Fertigstellung, ID der Softwarekomponenten, ID des Softwareoperationsszenarios, TID, PID, Funktionsaufrufadressen), Informationen zu den zu überprüfenden Netzwerkverbindungen (URL, Richtung der Verbindung, Größe des Netzwerkpakets), Informationen zu PDB-Dateien (Name, ID, Bildgröße der ausführbaren Datei), Informationen über zu prüfende Dateien (Name, vollständiger Pfad, Prüfsumme), Überwachungsparameter der Softwareleistung.

- Informationen über den letzten fehlgeschlagenen Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts seit der Installation des Betriebssystems, Daten zum System-Dump (Code und Parameter des Fehlers, Name, Version und Prüfsumme (CRC32) des Moduls, welches den Fehler bei der Arbeit des Betriebssystem hervorgerufen hat, Fehleradresse als Offset im Modul, Prüfsummen (MD5, SHA2-256, SHA1) des System-Dumps).

- Informationen für die Authentizitätsprüfung der Zertifikate, mit welchen die Dateien signiert sind: Fingerabdruck des Zertifikats, Algorithmus zur Berechnung der Prüfsumme, öffentlicher Schlüssel und Seriennummer des Zertifikats, Name des Zertifikatausstellers, Ergebnis der Zertifikatuntersuchung und ID der Zertifikatdatenbank;

- Informationen zum Prozess, welcher einen Angriff auf den Selbstschutz der Software ausgeführt hat: Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1), vollständiger Pfad und Code der Pfadvorlage der Prozessdatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung der Prozessdatei, Merkmal der ausführbaren Datei, Attribute der Prozessdatei, Informationen zum Zertifikat, mit welchem die Prozessdatei signiert ist, Code des Benutzerkontos, in deren Namen der Prozess gestartet wurde, ID der Vorgänge, welche für den Zugriff auf den Prozess ausgeführt wurden, Typ der Ressourcen, von welchen der Vorgang ausgeführt wurde (Prozess, Datei, Registrierungsobjekt, Suche des Fensters mithilfe der Funktion FindWindow), Name der Ressource, mit welcher der Vorgang ausgeführt wird, Merkmal für die erfolgreiche Ausführung des Vorgangs, Status der Prozessdatei und ihr Status in KSN;

- Informationen über die Software des Rechteinhabers: Vollversion, Typ, Lokalisierung und Betriebszustand der verwendeten Software, Versionen der installierten Software-Komponenten und deren Betriebszustand, Informationen über die installierten Software-Updates, den Wert des TARGET-Filters, die Version des für die Verbindung zu den Diensten des Rechteinhabers verwendeten Protokolls;

- Informationen über die Hardware, welche auf dem Computer installiert ist: Typ, Name, Modell, Firmware-Version, Merkmale von integrierten und verbundenen Geräten, einmalige ID des Computers, auf welchem die Software installiert ist.

- Informationen über die Versionen des Betriebssystems und der installierten Updates, Bit-Version, Edition und Einstellungen für den Ausführungsmodus des Betriebssystems, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems und Datum und Uhrzeit, an dem das Betriebssystem gestartet wurde;

- Ausführbare und nicht ausführbare Dateien, entweder ganz oder teilweise;

- Abschnitte aus dem Arbeitsspeicher des Computers;

- Sektoren, die am Ladeprozess des Betriebssystems beteiligt sind
- Datenpakete des Netzwerkverkehrs
- Webseiten und E-Mail-Nachrichten, die verdächtige und schädliche Objekte enthalten
- Beschreibung der Klassen und Exemplarklassen des WMI-Speichers
- Berichte über Aktivitäten der Programme:
  - Name, Größe und Version der gesendeten Datei, ihre Beschreibung und Prüfsummen (MD5, SHA2-256, SHA1), Kennung des Dateiformats, Name des Anbieters der Datei, Name des Produkts, zu dem die Datei gehört, vollständiger Pfad zu der Datei auf dem Computer, Vorlagencode des Pfads, Erstellungs- und Änderungszeitstempel der Datei;
  - Anfangs- und Enddatum/-zeit der Gültigkeitsdauer des Zertifikats (wenn die Datei eine digitale Signatur aufweist), Datum und Uhrzeit der Signatur, Name des Ausstellers des Zertifikats, Informationen über den Zertifikatsinhaber, Fingerabdruck, öffentlicher Schlüssel des Zertifikats und entsprechende Algorithmen sowie Seriennummer des Zertifikats;
  - Name des Kontos, von dem aus der Prozess ausgeführt wird;
  - Prüfsummen (MD5, SHA2-256, SHA1) des Namens des Computers, auf dem der Prozess läuft;
  - Titel der Prozessfenster;
  - ID der Antiviren-Datenbanken, Name der erkannten Bedrohung gemäß der Klassifizierung des Rechteinhabers;
  - Daten über die installierte Lizenz, deren ID, Typ und Ablaufdatum;
  - Ortszeit des Computers zum Zeitpunkt der Informationsbereitstellung;
  - Name und Pfade der Dateien, auf die der Prozess zugegriffen hat;
  - Name der Registrierungsschlüssel und ihrer Werte, auf die der Prozess zugegriffen hat;
  - URL und IP-Adressen, auf die durch den Prozess zugegriffen wurde;
  - URL und IP-Adressen, von denen die laufende Datei heruntergeladen wurde.

Einhaltung der Gesetzgebung der Europäischen Union (DSGVO)

Kaspersky Endpoint Security kann unter den folgenden Szenarien Daten an Kaspersky übertragen:

- Arbeiten mit dem Kaspersky Security Network
- Aktivieren des Programms mit einem Aktivierungscode
- Aktualisierung von Programm-Modulen und Antiviren-Datenbanken
- Folgende Links in der Programmoberfläche
- Aufzeichnung von Dump-Dateien

Unabhängig von der Datenklassifikation und dem Territorium, aus dem die Daten stammen, hält Kaspersky hohe Standards für die Datensicherheit ein und setzt verschiedene rechtliche, organisatorische und technische Maßnahmen ein, um die Daten der Benutzer zu schützen, die Datensicherheit und Vertraulichkeit zu gewährleisten und auch die Erfüllung der durch die geltende Gesetzgebung garantierten Rechte der Benutzer sicherzustellen. Der Text der Datenschutzrichtlinie ist im Leistungsumfang des Programms enthalten und auf der Kaspersky-Website verfügbar.

Bevor Sie Kaspersky Endpoint Security verwenden, lesen Sie bitte sorgfältig die Beschreibung zu den übertragenen Daten im Endbenutzer-Lizenzvertrag und in der KSN-Erklärung. Wenn bestimmte Daten, die von Kaspersky Endpoint Security unter einem der beschriebenen Szenarien übertragen werden, gemäß Ihrer lokalen Gesetzgebung oder Norm als personenbezogene Daten eingestuft werden können, müssen Sie sicherstellen, dass diese Daten rechtmäßig verarbeitet werden und die Zustimmung der Endbenutzer für die Erfassung und Übertragung dieser Daten einholen.

Ausführliche Angaben darüber, wie Informationen über die Programmverwendung empfangen, verarbeitet, gespeichert und gelöscht werden, nachdem der Lizenzvertrag und die Erklärung zu Kaspersky Security Network akzeptiert worden sind, finden Sie in den genannten Dokumenten und auf der Kaspersky-Website. Die Dateien license.txt und ksn_<ID der Sprache>.txt mit den Texten des Endbenutzer-Lizenzvertrags und der Erklärung zu Kaspersky Security Network gehören zum Lieferumfang des Programms.

Wenn Sie keine Daten an Kaspersky übertragen möchten, können Sie die Datenbereitstellung deaktivieren.

Arbeiten mit dem Kaspersky Security Network

Durch die Nutzung des Kaspersky Security Network erklären Sie sich damit einverstanden, die in der KSN-Erklärung aufgeführten Daten automatisch zur Verfügung zu stellen. Wenn Sie nicht damit einverstanden sind, Kaspersky diese Daten zur Verfügung zu stellen, verwenden Sie Private KSN oder deaktivieren Sie die Verwendung von KSN. Details über die Funktionsweise von Private KSN finden Sie in der *Dokumentation zu Kaspersky Private Security Network*.

Aktivieren des Programms mit einem Aktivierungscode

Durch die Verwendung eines Aktivierungscodes erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Wenn Sie es ablehnen, Kaspersky diese Informationen bereitzustellen, muss für die Aktivierung von Kaspersky Endpoint Security eine Schlüsseldatei verwendet werden.

Aktualisierung von Programm-Modulen und Antiviren-Datenbanken

Durch die Verwendung von Kaspersky-Servern erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Kaspersky benötigt diese Informationen, um zu überprüfen, ob Kaspersky Endpoint Security rechtmäßig verwendet wird. Wenn Sie nicht damit einverstanden sind, diese Informationen an Kaspersky weiterzugeben, verwenden Sie das Kaspersky Security Center für Datenbanken-Updates oder das Kaspersky Update-Dienstprogramm.

Folgende Links in der Programmoberfläche

Durch die Verwendung von Links in der Programmoberfläche erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Die genaue Liste der in jeder spezifischen Verbindung übertragenen Daten hängt davon ab, wo sich die Verbindung in der Programmoberfläche befindet und welches Problem damit gelöst werden soll. Wenn Sie nicht damit einverstanden sind, diese Daten Kaspersky zur Verfügung zu stellen, verwenden Sie die vereinfachte Programmoberfläche oder blenden Sie die Programmoberfläche aus.

Aufzeichnung von Dump-Dateien

Wenn Sie das Schreiben von Dump-Dateien aktiviert haben, erstellt Kaspersky Endpoint Security eine Dump-Datei, die alle Speicherdaten von Programmprozessen zum Zeitpunkt der Erstellung dieser Dump-Datei enthält.

Erste Schritte

Nach der Installation von Kaspersky Endpoint Security können Sie das Programm mithilfe der folgenden Schnittstellen verwalten:

- Lokale Programmoberfläche.
- Kaspersky Security Center Verwaltungskonsole.
- Kaspersky Security Center 12 Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Verwaltungskonsole

Mit Kaspersky Security Center können folgende Funktionen ferngesteuert werden: Kaspersky Endpoint Security installieren und entfernen, starten und beenden; Programmeinstellungen anpassen, Auswahl der Programmkomponenten ändern, Schlüssel hinzufügen, Update- und Untersuchungsaufgaben starten und beenden.

Das Programm Kaspersky Security Center wird mithilfe des Verwaltungs-Plug-ins von Kaspersky Endpoint Security verwaltet.

Weitere Informationen zur Verwaltung des Programms über Kaspersky Security Center *finden Sie in der Hilfe zu Kaspersky Security Center*.

Kaspersky Security Center 12 Web Console oder Kaspersky Security Center Cloud Console.

Kaspersky Security Center 12 Web Console (im Folgenden auch "*Web Console*") ist ein Programm (Web-Anwendung), mit dem grundlegende Aufgaben für die Verwaltung und Wartung des Schutzsystems eines Unternehmensnetzwerks zentralisiert gelöst werden können. "Web Console" ist eine Komponente von Kaspersky Security Center, die eine Benutzerschnittstelle bietet. Ausführliche Informationen über Kaspersky Security Center 12 Web Console finden Sie in der *Hilfe für Kaspersky Security Center*.

Kaspersky Security Center Cloud Console (im Folgenden "*Cloud Console*") ist eine Cloud-Lösung für den Schutz und die Kontrolle eines Unternehmensnetzwerks. Ausführliche Informationen über Kaspersky Security Center Cloud Console *finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console*.

Mithilfe von Web Console und Cloud Console können Sie die folgenden Aktionen ausführen:

- Status des Sicherheitssystems Ihres Unternehmens kontrollieren
- Kaspersky-Programme auf den Geräten Ihres Netzwerks installieren
- Installierte Programme verwalten
- Berichte über den Zustand des Sicherheitssystems einsehen

Die Verwaltung des Programms Kaspersky Endpoint Security über Web Console, Cloud Console und über die Verwaltungskonsole von Kaspersky Security Center weist Unterschiede auf. Auch die jeweilige Liste der verfügbaren Komponenten und Aufgaben unterscheidet sich.

Über das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows gewährleistet die Interaktion von Kaspersky Endpoint Security mit Kaspersky Security Center. Mithilfe des Verwaltungs-Plug-ins kann Kaspersky Endpoint Security für Windows unter Verwendung der folgenden Tools verwaltet werden: Richtlinien, Aufgaben und lokale Programmeinstellungen. Für die Interaktion mit „Kaspersky Security Center 12 Web Console“ ist ein Web-Plug-in vorgesehen.

Die Version des Verwaltungs-Plug-ins kann sich von der Version des Programms Kaspersky Endpoint Security unterscheiden, die auf dem Client-Computer installiert ist. Verfügt die installierte Version des Verwaltungs-Plug-ins über weniger Funktionen als die installierte Version von Kaspersky Endpoint Security, so werden die fehlenden Funktionen nicht mit dem Verwaltungs-Plug-in verwaltet. Diese Einstellungen können vom Benutzer in der lokalen Oberfläche von Kaspersky Endpoint Security geändert werden.

Das Web-Plug-in ist standardmäßig nicht in Kaspersky Security Center 12 Web Console installiert. Im Unterschied zum Verwaltungs-Plug-in für die „Verwaltungskonsole“ von Kaspersky Security Center, das am Administrator-Arbeitsplatz installiert wird, muss das Web-Plug-in auf einem Computer installiert werden, auf dem das Programm Kaspersky Security Center 12 Web Console installiert ist. Dabei sind die Funktionen des Web-Plug-ins für alle Administratoren verfügbar, die Zugriff auf „Web Console“ im Browser haben. Sie können auf der Benutzeroberfläche von „Web Console“ (**Einstellungen der Konsole** → **Plug-ins**) eine Liste der installierten Web-Plug-ins einsehen. Details über die Kompatibilität der Versionen des Web-Plug-ins mit „Web Console“ finden Sie in der *Hilfe für Kaspersky Security Center*.

Installation des Web-Plug-ins

Es gibt folgende Möglichkeiten, um das Web-Plug-in zu installieren:

- Web-Plug-in mithilfe des Schnellstartassistenten für Kaspersky Security Center 12 Web Console installieren.

  “Web Console“ schlägt bei der ersten Verbindung von „Web Console“ mit dem Administrationsserver automatisch vor, den Schnellstartassistenten zu starten. Außerdem können Sie den Schnellstartassistenten auf der Benutzeroberfläche von „Web Console“ starten (**Gerätesuche und Verteilung** → **Verteilung und Zuweisung** → **Schnellstartassistent**). Der Schnellstartassistent kann auch überprüfen, ob die installierten Web-Plug-ins aktuell sind, und kann die dafür erforderlichen Updates herunterladen. Details über den Schnellstartassistenten für Kaspersky Security Center 12 Web Console finden Sie in der *Hilfe für Kaspersky Security Center*.

- Installieren des Web-Plug-ins aus der Liste der verfügbaren Programmpakete in „Web Console“.

  Für die Installation des Web-Plug-ins muss das Programmpaket des Web-Plug-ins für Kaspersky Endpoint Security auf der Benutzeroberfläche von „Web Console“ ausgewählt werden (**Einstellungen der Konsole** → **Plug-ins**). Die Liste der verfügbaren Programmpakete wird automatisch aktualisiert, wenn neue Versionen von Kaspersky-Programmen erscheinen.

- Download des Programmpakets von einer externen Quelle in die „Web Console“.

  Für die Installation des Web-Plug-ins muss das ZIP-Archiv des Programmpakets für das Web-Plug-in von Kaspersky Endpoint Security auf der Benutzeroberfläche von „Web Console“ hinzugefügt werden (**Einstellungen der Konsole** → **Plug-ins**). Das Programmpaket des Web-Plug-ins können Sie beispielsweise von der Kaspersky-Website herunterladen.

Upgrade des Verwaltungs-Plug-ins

Um das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows zu aktualisieren, muss die neueste Version des Verwaltungs-Plug-ins geladen werden (sie gehört zum Lieferumfang) und der Plug-in-Installationsassistent muss ausgeführt werden.

Wenn eine neue Version des Web-Plug-ins für „Web Console“ verfügbar ist, wird die Benachrichtigung *Updates für die verwendeten Plug-ins sind verfügbar* angezeigt. Sie können aus der „Web Console“-Benachrichtigung zum Upgrade des Web-Plug-ins wechseln. Auf der Benutzeroberfläche von „Web Console“ (**Einstellungen der Konsole** → **Plug-ins**) können Sie auch manuell prüfen, ob Updates für das Web-Plug-in vorliegen. Im Verlauf des Updates wird die vorhergehende Version des Web-Plug-ins automatisch entfernt.

Beim Update des Web-Plug-ins werden bereits vorhandene Elemente (z. B. Richtlinien oder Aufgaben) gespeichert. Neue Einstellungen für Elemente, die neue Funktionen von Kaspersky Endpoint Security realisieren, erscheinen in den vorhandenen Elementen und besitzen Standardwerte.

Es gibt folgende Möglichkeiten, um das Web-Plug-in zu aktualisieren:

- Web-Plug-in in der Liste der Web-Plug-ins im Online-Modus aktualisieren.

  Für das Update des Web-Plug-ins muss das Programmpaket des Web-Plug-ins für Kaspersky Endpoint Security auf der Benutzeroberfläche von „Web Console“ ausgewählt und das Update gestartet werden (**Einstellungen der Konsole** → **Plug-ins**). “Web Console“ prüft, ob auf den Kaspersky-Servern Updates vorliegen und lädt die erforderlichen Updates herunter.

- Web-Plug-in aus einer Datei aktualisieren.

  Für das Update des Web-Plug-ins muss das ZIP-Archiv des Programmpakets für das Web-Plug-in von Kaspersky Endpoint Security auf der Benutzeroberfläche von „Web Console“ ausgewählt werden (**Einstellungen der Konsole** → **Plug-ins**). Das Programmpaket des Web-Plug-ins können Sie beispielsweise von der Kaspersky-Website herunterladen. Sie können das Web-Plug-in für Kaspersky Endpoint Security nur auf die neueste Version aktualisieren. Eine Aktualisierung des Web-Plug-ins auf eine ältere Version ist nicht möglich.

Wenn ein beliebiges Element geöffnet wird (z. B. eine Richtlinie oder eine Aufgabe), überprüft das Web-Plug-in die Kompatibilitätsinformationen. Wenn die Version des Web-Plug-ins mit der in den Kompatibilitätsinformationen angegeben Version übereinstimmt oder höher ist, können Sie die Einstellungen dieses Elements ändern. Andernfalls kann das ausgewählte Element nicht mithilfe des Web-Plug-ins geändert werden. Es wird empfohlen, das Web-Plug-in zu aktualisieren.

Besonderheiten für die Verwendung unterschiedlicher Versionen des Verwaltungs-Plug-ins

Sie können Kaspersky Endpoint Security nur dann über das Kaspersky Security Center verwalten, wenn Sie über ein Verwaltungs-Plug-In verfügen, dessen Version gleich oder höher ist als die Version, die in den Informationen zur Kompatibilität von Kaspersky Endpoint Security mit dem Verwaltungs-Plug-In angegeben ist. Die minimal erforderliche Version des Verwaltungs-Plug-Ins können Sie in der Datei installer.ini einsehen, die im Lieferumfang enthalten ist.

Wenn ein beliebiges Element geöffnet wird (z. B. eine Richtlinie oder eine Aufgabe), überprüft das Verwaltungs-Plug-in die Kompatibilitätsinformationen. Wenn die Version des Verwaltungs-Plug-ins mit der in den Kompatibilitätsinformationen angegeben Version übereinstimmt oder höher ist, können Sie die Einstellungen dieses Elements ändern. Andernfalls kann das gewählte Element mithilfe des Verwaltungs-Plug-ins nicht geändert werden. Es wird empfohlen, das Verwaltungs-Plug-in zu aktualisieren.

Update des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 10 für Windows”

Wenn in der Verwaltungskonsole das Verwaltungs-Plug-in für Kaspersky Endpoint Security 10 für Windows installiert ist, gelten für die Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security 11 für Windows folgende Besonderheiten:

- Das „Verwaltungs-Plug-in für Kaspersky Endpoint Security 10 für Windows“ wird nicht entfernt und bleibt verfügbar. Darum haben Sie Zugriff auf zwei Verwaltungs-Plug-ins für die Arbeit mit den Programmversionen 10 und 11.
- Das „Verwaltungs-Plug-in für Kaspersky Endpoint Security 11 für Windows“ unterstützt die Verwaltung des Programms Kaspersky Endpoint Security 10 für Windows auf den Benutzercomputern nicht.
- Elemente (z. B. Richtlinien oder Aufgaben), die mithilfe des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 10 für Windows“ erstellt wurden, werden vom „Verwaltungs-Plug-in für Kaspersky Endpoint Security 11 für Windows“ nicht unterstützt.

  Sie können den „Assistenten für die Konvertierung von Richtlinien und Aufgaben“ verwenden, um Richtlinien und Aufgaben von Version 10 auf Version 11 zu konvertieren. Details zum Konvertieren von Richtlinien und Aufgaben finden Sie in der *Hilfe zu Kaspersky Security Center*.

Update des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 11 für Windows”

Wenn in der „Verwaltungskonsole“ das „Verwaltungs-Plug-in für Kaspersky Endpoint Security 11 für Windows“ installiert ist, gelten für die Installation der neuen Version des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 11 für Windows“ folgende Besonderheiten:

- Die ältere Version des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 11 für Windows“ wird entfernt.
- Die neue Version des „Verwaltungs-Plug-ins für Kaspersky Endpoint Security 11 für Windows“ unterstützt die Verwaltung der älteren Version des Programms Kaspersky Endpoint Security 11 für Windows auf den Benutzercomputern nicht.
- Sie können mithilfe der neuen Version des Verwaltungs-Plug-ins die Einstellungen in Richtlinien, Aufgaben usw. ändern, die mit der älteren Version des Verwaltungs-Plug-ins erstellt wurden.
- Für neue Einstellungen werden von der neuen Version des Verwaltungs-Plug-ins die Standardwerte festgelegt, sobald eine Richtlinie, ein Richtlinienprofil oder eine Aufgabe zum ersten Mal gespeichert wird.

  Es wird empfohlen, nach dem Update des Verwaltungs-Plug-ins die Werte der neuen Einstellungen in den Richtlinien und Richtlinienprofilen zu überprüfen und zu speichern. Sollten Sie dies nicht tun, so besitzen die neuen Einstellungsblöcke von Kaspersky Endpoint Security auf dem Benutzercomputer die Standardwerte und können geändert werden (Attribut). Mit der Überprüfung sollte bei den Richtlinien und Richtlinienprofilen der höheren Ebene einer Hierarchie begonnen werden. Außerdem wird empfohlen, ein Benutzerkonto zu verwenden, für das Zugriffsrechte auf alle funktionalen Bereich von Kaspersky Security Center vorhanden sind.

  Über neue Programmfunktionen können Sie sich in den Versionshinweisen oder in der Hilfe zum Programm informieren.

- Wenn in der neuen Version des Verwaltungs-Plug-ins eine neue Einstellung zu einem Einstellungsblock hinzugefügt wurde, bleibt der Status des Attributs / für diesen Einstellungsblock unverändert.

- Wenn Sie das Verwaltungs-Plug-in auf Version 11.2.0 upgraden, müssen Sie eine Richtlinie öffnen, um sie automatisch zu konvertieren. Bei diesem Vorgang fordert Kaspersky Endpoint Security Sie auf, die Teilnahme an KSN zu bestätigen. Wenn Sie für das Programm bereits auf anderen Computern Ihres Unternehmens ein Upgrade auf Version 11.20 durchgeführt haben, wird die Teilnahme an KSN deaktiviert, bis Sie die KSN-Teilnahmebedingungen akzeptieren.

Besondere Überlegungen bei der Verwendung verschlüsselter Protokolle für die Interaktion mit externen Diensten

Kaspersky Endpoint Security und Kaspersky Security Center verwenden einen verschlüsselten Kommunikationskanal mit TLS (Transport Layer Security), um mit externen Diensten von Kaspersky zusammenzuarbeiten. Kaspersky Endpoint Security verwendet externe Dienste für die folgenden Funktionen:

- Update der Datenbanken und Programm-Module
- Aktivierung des Programms mit einem Aktivierungscode (Aktivierung 2.0)
- Verwendung von Kaspersky Security Network

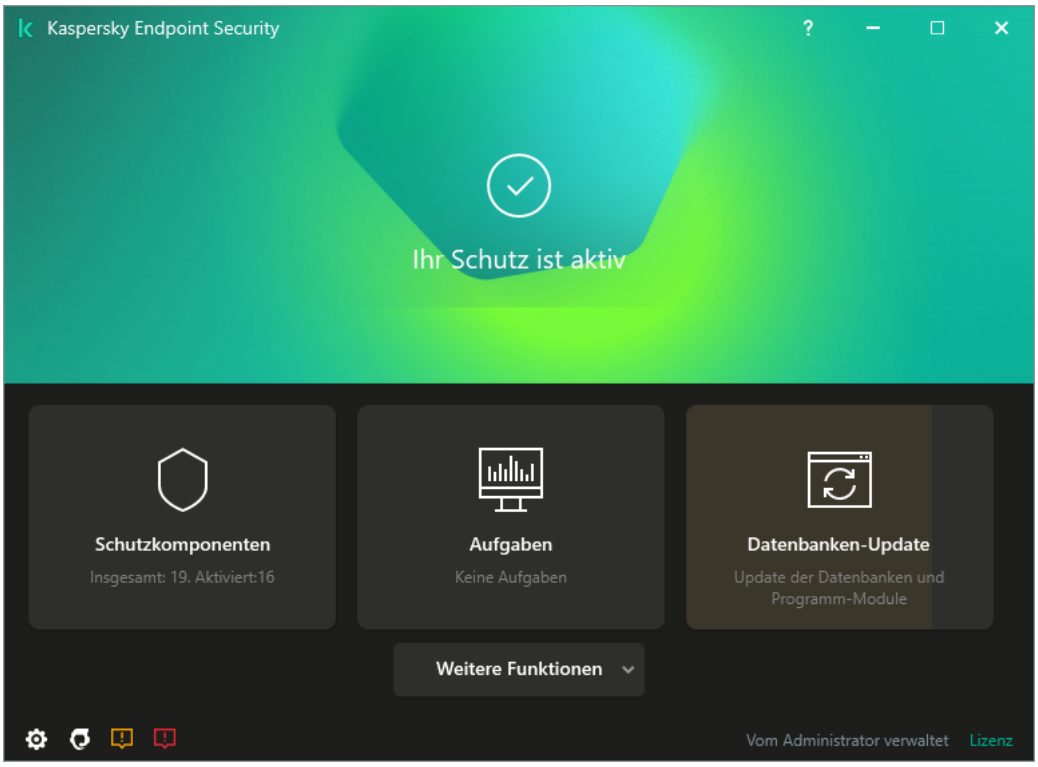
Die Verwendung von TLS sichert das Programm durch die Bereitstellung der folgenden Funktionen:

- Verschlüsselung. Der Inhalt der Nachrichten ist vertraulich und wird nicht an Drittnutzer weitergegeben.
- Integrität. Der Empfänger der Nachricht ist sicher, dass der Inhalt der Nachricht seit der Weiterleitung durch den Absender nicht geändert wurde.
- Authentifizierung. Der Empfänger ist sicher, dass die Kommunikation nur mit einem vertrauenswürdigen Kaspersky-Server hergestellt wird.

Kaspersky Endpoint Security verwendet Zertifikate mit öffentlichen Schlüsseln zur Serverauthentifizierung. Für die Arbeit mit Zertifikaten ist eine Infrastruktur für öffentliche Schlüssel (PKI, Public Key Infrastructure) erforderlich. Eine Zertifizierungsstelle ist Teil einer PKI. Kaspersky verwendet seine eigene Zertifizierungsstelle, da die Kaspersky-Dienste hochtechnisch und nicht öffentlich sind. Wenn Stammzertifikate von Thawte, VeriSign, GlobalTrust und anderen widerrufen werden, bleibt die Kaspersky-PKI in diesem Fall weiterhin betriebsbereit.

Umgebungen, die über MITM (Software- und Hardware-Tools, die das Parsen des HTTPS-Protokolls unterstützen) verfügen, werden von Kaspersky Endpoint Security als unsicher eingestuft. Bei der Arbeit mit Kaspersky-Diensten können Fehler auftreten. Beispielsweise kann es Fehler bei der Verwendung von selbstsignierten Zertifikaten geben. Diese Fehler können auftreten, weil ein HTTPS-Inspektionstool aus Ihrer Umgebung die Kaspersky PKI nicht erkennt. Um diese Probleme zu beheben, müssen Sie Ausnahmen für die Interaktion mit externen Diensten konfigurieren.

Programmoberfläche



Programmhauptfenster

Schutzkomponenten	Betriebsstatus der installierten Komponenten. Sie können auch mit der Konfiguration jeder der installierten Komponenten mit Ausnahme der Verschlüsselungskomponenten fortfahren.
Aufgaben	Die Untersuchungsaufgaben von Kaspersky Endpoint Security verwalten. Sie können eine Virensuche und eine Integritätsprüfung des Programms durchführen. Ein Administrator kann Aufgaben vor einem Benutzer verbergen oder die Verwaltung von Aufgaben einschränken.
Datenbanken-Update	Die Update-Aufgaben für Kaspersky Endpoint Security verwalten. Sie können Antiviren-Datenbanken und Programm-Module aktualisieren und das letzte Update zurücksetzen. Ein Administrator kann Aufgaben vor einem Benutzer verbergen oder die Verwaltung von Aufgaben einschränken.
Weitere Funktionen	Mit anderen Programmfunktionen fortfahren. • **Berichte**. Zeigen Sie Ereignisse an, die bei der Nutzung des Programms, einzelner Komponenten und Aufgaben aufgetreten sind. • **Backup**. Eine Liste der gespeicherten Kopien von infizierten Dateien anzeigen, die vom Programm gelöscht wurden. • **Technologien zur Erkennung**. Hier finden Sie Informationen über Technologien zur Erkennung von Bedrohungen und die Anzahl der von diesen Technologien erkannten Bedrohungen. • **Kaspersky Security Network**. Status der Verbindung zwischen Kaspersky Endpoint Security und Kaspersky Security Network sowie globale KSN-Statistiken. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. Wenn Sie an Kaspersky Security Network teilnehmen, erhält das

	Programm Kaspersky Endpoint Security von den KSN-Diensten Informationen über die Kategorie und die Reputation untersuchter Dateien, sowie Informationen über die Reputation untersuchter Webadressen. • **Aktivitätsmonitor**. Informationen über den Betrieb der installierten Programme anzeigen. Der Aktivitätsmonitor überwacht Datei-, Registrierungs- und Systemereignisse, die im Betriebssystem auftreten und sich auf ein Programm beziehen. • **Netzwerkmonitor**. Informationen über die Netzwerkaktivität des Computers in Echtzeit anzeigen. • **Verschlüsselungsmonitor**. Überwacht den Vorgang der Festplattenverschlüsselung und -entschlüsselung in Echtzeit. Encryption Monitor ist verfügbar, wenn die Komponente „Kaspersky-Festplattenverschlüsselung“ oder „BitLocker-Laufwerkverschlüsselung“ installiert ist.
	Programmeinstellungen anpassen. Ein Administrator kann Änderungen an Einstellungen im Kaspersky Security Center verbieten.
	Informationen über das Programm: aktuelle Version von Kaspersky Endpoint Security, Datum der Veröffentlichung der Datenbank, Schlüssel und andere Informationen. Sie können auch zu den Kaspersky-Informationsquellen navigieren, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Kauf, zur Installation und zur Verwendung des Programms bieten.
/	Nachrichten, die Informationen über verfügbare Updates und Anträge auf Zugang zu verschlüsselten Dateien und Geräten enthalten.
Lizenz	Lizenzverwaltung des Programms. Sie können eine Lizenz erwerben, das Programm aktivieren oder ein Abonnement verlängern. Sie können auch Informationen über die aktuelle Lizenz anzeigen.

Programmsymbol im Infobereich

Sofort nach der Installation von Kaspersky Endpoint Security erscheint das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol übernimmt folgende Funktionen:

- Es dient als Indikator für die Ausführung des Programms.
- Es ermöglicht den Zugriff auf das Kontextmenü und auf das Programmhauptfenster.

Für das Programmsymbol gibt es die folgenden Statusvarianten, die Informationen über die Programmnutzung visualisieren:

- Das Symbol bedeutet, dass alle kritischen Schutzkomponenten des Programms aktiviert sind. Kaspersky Endpoint Security zeigt eine Warnung an, wenn der Benutzer eine Aktion ausführen muss, z. B. den Computer nach der Aktualisierung des Programms neu starten.
- Das Symbol bedeutet, dass die Funktion der Schutzkomponenten des Programms deaktiviert oder gestört ist. Die Funktion der Schutzkomponenten kann beispielsweise gestört sein, wenn die Lizenz abgelaufen ist oder

im Programm eine Störung aufgetreten ist. Kaspersky Endpoint Security zeigt die Warnung und eine Beschreibung des Problems im Computerschutz an.

Das Kontextmenü des Programmsymbols enthält die folgenden Punkte:

- **Kaspersky Endpoint Security für Windows**. Öffnet das Programmhauptfenster. In diesem Fenster können Sie die Funktion der Komponenten und Aufgaben des Programms anpassen sowie eine Statistik zu verarbeiteten Dateien und gefundenen Bedrohungen einsehen.

- **Schutz anhalten / Schutz fortsetzen**. Anhalten aller Schutz- und Kontrollkomponenten, die in der Richtlinie kein Vorhängeschloss () haben. Bevor dieser Vorgang ausgeführt wird, sollte die Richtlinie für Kaspersky Security Center deaktiviert werden.

  Bevor die Schutz- und Kontrollkomponenten angehalten werden, fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dann können Sie auswählen, wie lange die Pause dauern soll: für einen bestimmten Zeitraum, bis zum Neustart, oder Fortsetzung auf Befehl des Benutzers.

  Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um den Betrieb der Schutz- und Kontrollkomponenten wieder aufzunehmen, wählen Sie **Schutz fortsetzen** im Kontextmenü des Programms.

  > Das Anhalten der Schutz- und Kontrollkomponenten beeinflusst die Ausführung von Update- und Untersuchungsaufgaben nicht. Das Programm setzt auch die Verwendung von Kaspersky Security Network fort.

- **Richtlinie deaktivieren** / **Richtlinie aktivieren**. Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss () haben. Beim Deaktivieren der Richtlinie fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um die Richtlinie zu aktivieren, wählen Sie im Programm-Kontextmenü den Punkt **Richtlinie aktivieren** aus.

- Einstellungen. Öffnet das Fenster mit den Programmeinstellungen.

- **Support**. Öffnen des Fensters **Support**, das Informationen enthält, die zur Kontaktaufnahme mit dem Technischen Support von Kaspersky erforderlich sind.

- **Über das Programm**. Öffnet ein Informationsfenster mit Angaben zum Programm.

- **Beenden**. Beendet Kaspersky Endpoint Security. Wenn Sie diese Option im Kontextmenü gewählt haben, wird das Programm aus dem Arbeitsspeicher des Computers entfernt.

Kontextmenü des Programmsymbols

Einfache Programmoberfläche

Wenn der Client-Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie von Kaspersky Security Center unterliegt und in dieser Richtlinie die Anzeige der einfachen Programmoberfläche festgelegt ist, so ist das Programmhauptfenster auf diesem Client-Computer nicht verfügbar. Der Benutzer kann durch Rechtsklick das Kontextmenü des Symbols von Kaspersky Endpoint Security öffnen (siehe folgende Abb.), das folgende Punkte enthält:

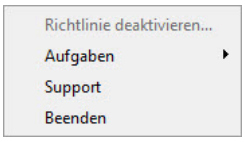
- **Richtlinie deaktivieren** / **Richtlinie aktivieren**. Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss () haben. Beim Deaktivieren der Richtlinie fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um die Richtlinie zu aktivieren, wählen Sie im Programm-Kontextmenü den Punkt **Richtlinie aktivieren** aus.

- **Aufgaben**. Dropdown-Liste mit folgenden Elementen:

  - **Integritätsprüfung**.
  - **Rollback des letzten Updates**
  - **Vollständige Untersuchung**.
  - **Benutzerdefinierte Untersuchung**.
  - **Untersuchung wichtiger Bereiche**.
  - **Update**.

- **Support**. Öffnen des Fensters **Support**, das Informationen enthält, die zur Kontaktaufnahme mit dem Technischen Support von Kaspersky erforderlich sind.

- **Beenden**. Beendet Kaspersky Endpoint Security. Wenn Sie diese Option im Kontextmenü gewählt haben, wird das Programm aus dem Arbeitsspeicher des Computers entfernt.



Kontextmenü des Programmsymbols bei der Anzeige der einfachen Programmoberfläche

Darstellung der Programmoberfläche anpassen

Sie können die Anzeige der Programmoberfläche für den Computerbenutzer anpassen. Der Benutzer kann wie folgt mit dem Programm interagieren:

- **Mit vereinfachter Programmoberfläche**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.

- **Mit vollständiger Programmoberfläche**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.

- **Ohne Programmoberfläche**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.

So konfigurieren Sie den Anzeigemodus der Programmoberfläche in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.
6. Führen Sie im Abschnitt **Interaktion mit dem Benutzer** eine der folgenden Aktionen aus:
   - Damit auf dem Client-Computer folgende Elemente der Benutzeroberfläche angezeigt werden, aktivieren Sie das Kontrollkästchen **Programmoberfläche anzeigen**:
     - Ordner mit dem Namen des Programms im **Start**menü
     - Symbol für Kaspersky Endpoint Security im Infobereich der Taskleiste von Microsoft Windows
     - Pop-up-Benachrichtigungen

     Ist dieses Kontrollkästchen aktiviert, so kann der Benutzer die Programmeinstellungen über die Programmoberfläche einsehen und bei vorliegender Berechtigung ändern.
   - Um auf dem Client-Computer alle Hinweise für die Arbeit von Kaspersky Endpoint Security zu verbergen, deaktivieren Sie das Kontrollkästchen **Programmoberfläche anzeigen**.
7. Damit auf dem Client-Computer, auf welchem das Programm Kaspersky Endpoint Security installiert ist, die einfache Programmoberfläche angezeigt wird, aktivieren Sie im Block **Interaktion mit dem Benutzer** das Kontrollkästchen **Einfache Programmoberfläche**.

So konfigurieren Sie den Anzeigemodus der Programmoberfläche in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Unterstützung des portablen Modus aktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
5. Passen Sie im Block **Interaktion mit dem Benutzer** die Anzeige der Benutzeroberfläche an:

   - **Mit vereinfachter Programmoberfläche**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.
   - **Mit vollständiger Programmoberfläche**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.
   - **Ohne Programmoberfläche**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.
6. Klicken Sie auf **OK**.

Erste Schritte

Nachdem das Programm auf den Client-Computern verteilt wurde, müssen Sie wie folgt vorgehen, um Kaspersky Endpoint Security aus Kaspersky Security Center zu verwenden:

- Richtlinie erstellen und anpassen.

  Mithilfe von Richtlinien können Sie identische Funktionseinstellungen von Kaspersky Endpoint Security für alle Client-Computer festlegen, die zu einer Administrationsgruppe gehören. Der Schnellstartassistent für Kaspersky Security Center erstellt automatisch eine Richtlinie für Kaspersky Endpoint Security.

- Aufgaben *Update* und *Untersuchung auf Viren* erstellen.

  Die Aufgabe *Update* ist erforderlich, um den Computerschutz auf dem neuesten Stand zu halten. Bei der Aufgabenausführung aktualisiert Kaspersky Endpoint Security die Antiviren-Datenbanken und die Programm-Module. Die Aufgabe *Update* wird vom Schnellstartassistenten für Kaspersky Security Center automatisch erstellt. Um die Aufgabe *Updates* zu erstellen, installieren Sie mithilfe des Assistenten das Web-Plug-in für Kaspersky Endpoint Security für Windows.

  Die *Untersuchung auf Viren* ist erforderlich, um Viren und andere bedrohliche Programme rechtzeitig zu erkennen. Die Aufgabe *Untersuchung auf Viren* müssen Sie manuell erstellen.

In der Verwaltungskonsole (MMC) eine Aufgabe zur Untersuchung auf Viren erstellen

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** → **Untersuchung auf Viren** aus.

Schritt 2. Untersuchungsbereich

Erstellen Sie eine Liste der Objekte, die Kaspersky Endpoint Security im Rahmen der Untersuchungsaufgabe untersuchen soll.

Schritt 3. Aktion von Kaspersky Endpoint Security

Wählen Sie die Aktion beim Fund einer Bedrohung aus:

- **Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht.

- **Desinfizieren; informieren, wenn Desinfektion nicht möglich**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.

- **Informieren** Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.

- **Aktive Desinfektion sofort ausführen**. Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security bei der Untersuchung die Technologie zur aktiven Desinfektion.

  Die *Technologie zur Desinfektion aktiver Infektionen* dient dazu, schädliche Programme aus dem Betriebssystem zu entfernen, falls diese ihre Prozesse bereits im Arbeitsspeicher gestartet haben und Kaspersky Endpoint Security daran hindern, sie auf reguläre Weise zu neutralisieren. Dadurch wird die Bedrohung neutralisiert. Es wird davon abgeraten, während der aktiven Desinfektion neue Prozesse zu starten oder die Registrierung des Betriebssystems zu ändern. Die Technologie zur Desinfektion aktiver Infektionen beansprucht erhebliche Betriebssystemressourcen, wodurch die Ausführung anderer Programme verlangsamt werden kann. Nach Abschluss der aktiven Desinfektion startet Kaspersky Endpoint Security den Computer neu, ohne nach einer Bestätigung des Benutzers zu fragen.

Passen Sie den Startmodus für die Untersuchung mithilfe des Kontrollkästchens **Nur bei Computerleerlauf ausführen** an. Dieses Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit der die Aufgabe *Virensuche* angehalten wird, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security hält die Aufgabe *Virensuche* an, wenn der Bildschirmschoner nicht aktiviert und der Computer entsperrt ist.

Schritt 4. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 5: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie eine Benutzerkonto für den Start der Aufgabe *Virensuche* aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos. Wenn zum Untersuchungsbereich Netzlaufwerke oder andere Objekte gehören, auf die der Zugriff beschränkt ist, wählen Sie ein Benutzerkonto mit den erforderlichen Zugriffsrechten aus.

Schritt 6. Zeitplan des Aufgabenstarts anpassen

Passen Sie einen Zeitplan für den Aufgabenstart an, beispielsweise manuell oder nachdem die Antiviren-Datenbanken in den Speicher geladen wurden.

Schritt 7. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen an, beispielsweise `Vollständige Untersuchung täglich`.

Schritt 8. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch wird auf den Benutzercomputern eine Virensuche gemäß dem festgelegten Zeitplan ausgeführt.

[So erstellen Sie eine Aufgabe für eine Untersuchung auf Viren in der Web Console]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Variante **Untersuchung auf Viren** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Wöchentliche Untersuchung`.

   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertig**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Wechseln Sie zu den Aufgabeneigenschaften, um den Zeitplan für die Aufgabenausführung anzupassen.

   Die Ausführung der Aufgabe sollte mindestens einmal wöchentlich eingeplant werden.

7. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

8. Klicken Sie auf **Starten**.

   Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

Dadurch wird auf den Benutzercomputern eine Virensuche gemäß dem festgelegten Zeitplan ausgeführt.

Richtlinienverwaltung

Eine *Richtlinie* ist eine Auswahl von Programmeinstellungen, die für eine bestimmte Administrationsgruppe gilt. Für ein Programm können mehrere Richtlinien mit unterschiedlichen Werten angepasst werden. Die Programmeinstellungen können sich für bestimmte Administrationsgruppen unterscheiden. In jeder Administrationsgruppe kann eine eigene Richtlinie für das Programm erstellt werden.

Die Einstellungen der Richtlinie werden bei der *Synchronisierung* mithilfe des Administrationsagenten an die Client-Computer übertragen. Standardmäßig führt der Administrationsserver die Synchronisierung sofort aus, nachdem die Einstellungen der Richtlinie geändert wurden. Die Synchronisierung erfolgt über den UDP-Port 15000 auf dem Client-Computer. Der Administrationsserver führt standardmäßig alle 15 Minuten eine Synchronisierung durch. Wenn eine Synchronisierung nach der Änderung der Richtlinieneinstellungen fehlgeschlagen ist, wird der nächste Synchronisierungsversuch nach dem vorgegebenen Zeitplan ausgeführt.

Aktive und inaktive Richtlinie

Eine Richtlinie ist für eine Gruppe von verwalteten Computern vorgesehen und kann entweder aktiv oder inaktiv sein. Die Einstellungen einer aktiven Richtlinie werden bei der Synchronisierung auf den Client-Computern gespeichert. Für einen Computer dürfen nicht mehrere Richtlinien gleichzeitig gelten, deshalb kann in jeder Gruppe nur eine Richtlinie aktiv sein.

Sie können unbeschränkt viele inaktive Richtlinien erstellen. Eine inaktive Richtlinie beeinflusst die Programmeinstellungen auf den Computern im Netzwerk nicht. Inaktive Richtlinien erlauben eine schnelle Reaktion auf Extremsituationen wie beispielsweise Virenangriffe. Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. Dabei wird die aktive Richtlinie automatisch inaktiv.

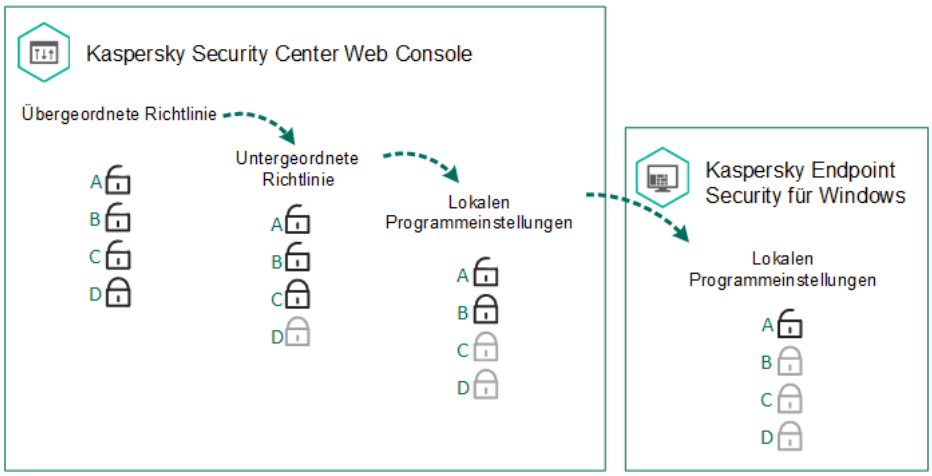
Mobile Richtlinie

Die mobile Richtlinie wird aktiviert, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.

Vererbung von Einstellungen

Richtlinien und Administrationsgruppen sind hierarchisch organisiert. Eine untergeordnete Richtlinie erbt standardmäßig die Einstellungen der übergeordneten Richtlinie. Eine *untergeordnete Richtlinie* ist die Richtlinie einer untergeordneten Hierarchie-Ebene, d. h. eine Richtlinie für untergeordnete Administrationsgruppen und sekundäre Administrationsserver. Sie können die Vererbung von Einstellungen aus der übergeordneten Richtlinie deaktivieren.

Jede Einstellung, die in einer Richtlinie enthalten ist, besitzt das Attribut . Es zeigt an, ob das Ändern von Einstellungen in den untergeordneten Richtlinien und in den lokalen Programmeinstellungen verboten ist. Das Attribut funktioniert nur, wenn in der untergeordneten Richtlinie die Vererbung von Einstellungen aus der übergeordneten Richtlinie aktiviert ist. Mobile Richtlinien unterliegen nicht der Hierarchie von Administrationsgruppen für andere Richtlinien.



Vererbung von Einstellungen

Die Rechte für den Zugriff auf Richtlinieneinstellungen (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Administrationsserver für Kaspersky Security Center besitzt, und zudem separat für jeden Funktionsbereich von Kaspersky Endpoint Security. Um die Rechte für den Zugriff auf die Richtlinieneinstellungen anzupassen, gehen Sie im Eigenschaftenfenster des Kaspersky Security Center-Administrationsservers zum Abschnitt **Sicherheit**.

Richtlinie erstellen

Erstellen einer Richtlinie In der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die entsprechenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Klicken Sie auf die Schaltfläche **Neue Richtlinie**.

   Der Assistent für neue Richtlinien wird gestartet.
5. Folgen Sie den Anweisungen des Assistenten für neue Richtlinien.

So erstellen Sie eine Richtlinie in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Richtlinien wird gestartet.
3. Wählen Sie das Programm Kaspersky Endpoint Security aus und klicken Sie auf **Weiter**.
4. Lesen und akzeptieren Sie die „Erklärung zu Kaspersky Security Network“ (KSN) und klicken Sie auf **Weiter**.
5. Auf der Registerkarte **Allgemein** können Sie folgende Aktionen ausführen:
   - Name der Richtlinie ändern
   - Status der Richtlinie auswählen:
     - **Aktiv**. Die Richtlinie wird auf diesem Computer nach der nächsten Synchronisierung als aktive Richtlinie verwendet.
     - **Inaktiv**. Ersatzrichtlinie. Eine inaktive Richtlinie kann erforderlichenfalls aktiviert werden.
     - **Mobil**. Die Richtlinie wird nur wirksam, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.
   - Vererbung von Einstellungen anpassen:
     - **Einstellungen der übergeordneten Richtlinie erben**. Ist dieser Schalter aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Stufe übernommen. Die Einstellungen der Richtlinie können nicht geändert werden, wenn in der übergeordneten Richtlinie das Attribut gilt.
     - **Zwingendes Vererben von Einstellungen für untergeordnete Richtlinien gewährleisten**. Ist der Schalter aktiviert, so werden die Werte der Richtlinieneinstellungen an die untergeordnete Richtlinien vererbt. In den Eigenschaften der untergeordneten Richtlinie wird der Schalter **Einstellungen der übergeordneten Richtlinie erben** automatisch aktiviert und kann nicht mehr deaktiviert werden. Die Einstellungen der untergeordneten Richtlinie werden aus der übergeordneten Richtlinie übernommen, unter Ausnahme von Einstellungen mit dem Attribut . Die Einstellungen von untergeordneten Richtlinien können nicht geändert werden, wenn in der übergeordneten Richtlinie das Attribut gilt.
6. Auf der Registerkarte **Programmeinstellungen** können Sie die Einstellungen der Richtlinie für Kaspersky Endpoint Security anpassen.
7. Klicken Sie auf **Speichern**.

Dadurch wird festgelegt, dass die Einstellungen von Kaspersky Endpoint Security auf den Client-Computern bei der nächsten Synchronisierung angepasst werden. Informationen über die Richtlinie, die für den Computer gilt, können Sie auf der Benutzeroberfläche von Kaspersky Endpoint Security einsehen. Klicken Sie dazu auf dem Hauptbildschirm auf die Schaltfläche **Support** (z. B. Name der Richtlinie). Dafür muss in den Richtlinieneinstellungen des Administrationsagenten der Empfang erweiterter Richtliniendaten aktiviert sein. Details über die Richtlinie des Administrationsagenten finden Sie in der *Hilfe zu Kaspersky Security Center*.

Indikator des Schutzniveaus

Im oberen Bereich des Fensters **Eigenschaften: <Name der Richtlinie>** wird der Indikator des Schutzniveaus angezeigt. Der Indikator kann einen der folgenden Werte annehmen:

- **Hohes Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Grün, wenn alle Komponenten, die zu den folgenden Kategorien gehören, aktiviert sind:
  - **Kritisch**. Diese Kategorie umfasst die folgenden Komponenten:
    - Schutz vor bedrohlichen Dateien
    - Verhaltensanalyse.
    - Exploit-Prävention.
    - Rollback von schädlichen Aktionen
  - **Wichtig**. Diese Kategorie umfasst die folgenden Komponenten:
    - Kaspersky Security Network
    - Schutz vor Web-Bedrohungen.
    - Schutz vor E-Mail-Bedrohungen.
    - Programm-Überwachung.
- **Mittleres Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Gelb, wenn eine wichtige Komponente deaktiviert ist.
- **Niedriges Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Rot, wenn einer der folgenden Fälle eintritt:
  - Eine oder mehrere kritische Komponenten sind deaktiviert.
  - Eine oder mehrere wichtige Komponenten sind deaktiviert.

Wenn der Indikator mit dem Wert **Mittleres Schutzniveau** oder **Niedriges Schutzniveau** angezeigt wird, befindet sich rechts vom Indikator ein Link, der ins Fenster **Empfohlene Schutzkomponenten** führt. In diesem Fenster können Sie die empfohlenen Schutzkomponenten aktivieren.

Aufgabenverwaltung

Für die Arbeit mit Kaspersky Endpoint Security über Kaspersky Security Center können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben für einen einzelnen Client-Computer
- Gruppenaufgaben für Client-Computer, die zu Administrationsgruppen gehören
- Aufgabe für bestimmte Computer.

Sie können beliebig viele Gruppenaufgabe, Aufgaben für bestimmte Computer und lokale Aufgaben erstellen. Details über die Verwendung von Administrationsgruppen und bestimmten Computern *finden Sie in der Hilfe für Kaspersky Security Center*.

Kaspersky Endpoint Security unterstützt die Ausführung der folgenden Aufgaben:

- **Untersuchung auf Viren**. Kaspersky Endpoint Security untersucht die Computerbereiche, die in den Aufgabeneinstellungen angegeben sind, auf Viren und andere bedrohliche Programme. Die Aufgabe *Untersuchung auf Viren* ist für Kaspersky Endpoint Security obligatorisch und wird im Rahmen des Schnellstartassistenten erstellt. Die Ausführung der Aufgabe sollte mindestens einmal wöchentlich eingeplant werden.

- **Schlüssel hinzufügen**. Kaspersky Endpoint Security fügt einen Schlüssel für die Aktivierung des Programms hinzu. Dies kann auch ein Reserveschlüssel sein. Vergewissern Sie sich vor der Aufgabenausführung, dass die Anzahl der Computer, auf denen die Aufgabe ausgeführt werden soll, nicht über der Anzahl der Computer liegt, für welche die Lizenz gilt.

- **Auswahl der Programmkomponenten ändern**. Kaspersky Endpoint Security installiert oder löscht Komponenten auf den Client-Computern. Dabei wird nach der Komponentenliste verfahren, die in den Aufgabeneinstellungen angegeben ist. Die Komponente „Schutz vor bedrohlichen Dateien“ kann nicht gelöscht werden. Durch eine optimale Auswahl der Komponenten von Kaspersky Endpoint Security können die Ressourcen des Computers geschont werden.

- **Inventar**. Kaspersky Endpoint Security erhält Informationen über alle ausführbaren Programmdateien, die auf dem Computer gespeichert sind. Die Aufgabe *Inventar* wird von der Komponente „Programmkontrolle“ ausgeführt. Wenn die Komponente „Programmkontrolle“ nicht installiert ist, wird die Aufgabe mit einem Fehler beendet.

- **Update**. Kaspersky Endpoint Security aktualisiert die Datenbanken und Programm-Module. Die Aufgabe *Update* ist für Kaspersky Endpoint Security obligatorisch und wird im Rahmen des Schnellstartassistenten erstellt. Die Ausführung der Aufgabe sollte mindestens einmal täglich eingeplant werden.

- **Daten löschen**. Kaspersky Endpoint Security löscht die Dateien und Ordner vom Benutzercomputer entweder sofort oder wenn längere Zeit keine Verbindung zu Kaspersky Security Center besteht.

- **Update-Rollback**. Kaspersky Endpoint Security macht das letzte Update der Datenbanken und Programm-Module rückgängig. Dies kann beispielsweise erforderlich sein, wenn die neuen Datenbanken fehlerhafte Daten enthalten, was dazu führen kann, dass Kaspersky Endpoint Security ein sicheres Programm blockiert.

- **Integritätsprüfung**. Kaspersky Endpoint Security analysiert die Programmdateien, untersucht die Dateien auf Beschädigungen und Veränderungen, und überprüft die digitalen Signaturen der Programmdateien.

- **Authentifizierungsagenten-Konten verwalten**. Kaspersky Endpoint Security passt die Einstellungen der Benutzerkonten für den Authentifizierungsagenten an. Der Authentifizierungsagent ist für die Arbeit mit verschlüsselten Datenträgern erforderlich. Der Benutzer muss vor dem Start des Betriebssystems die Authentifizierung mithilfe des Agenten durchlaufen.

Die Aufgaben werden nur dann auf dem Computer gestartet, wenn das Programm Kaspersky Endpoint Security läuft.

Erstellen einer Aufgabe

In der Verwaltungskonsole (MMC) eine Aufgabe erstellen

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Aufgaben**.
3. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.
   Der Assistent für neue Aufgaben wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben.

So erstellen Sie eine Aufgabe in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.
   Der Assistent für neue Aufgaben wird gestartet.
3. Passen Sie die Einstellungen der Aufgabe an:
   a. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.
   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Aufgabe aus, die Sie auf den Benutzercomputern starten möchten.
   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Update des Buchhaltungsprogramms`.
   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.
4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.
5. Beenden Sie den Assistenten durch Klick auf **Fertig**.

Die neue Aufgabe wird in der Aufgabenliste angezeigt. Die Aufgabe besitzt Standardeinstellungen. Um die Aufgabeneinstellungen anzupassen, müssen Sie zu den Aufgabeneigenschaften wechseln. Um die Aufgabe auszuführen, aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**. Nach dem Aufgabenstart können Sie die Aufgabe anhalten und später fortsetzen.

In der Aufgabenliste können Sie das Ausführungsergebnis der Aufgaben kontrollieren: Aufgabenstatus und Statistik über die Aufgabenausführung auf den Computern. Sie können auch eine Auswahl mit bestimmten Ereignissen erstellen, um die Aufgabenausführung zu kontrollieren (**Monitoring und Berichte** → **Ereignisauswahlen**). Details über die Ereignisauswahl *finden Sie in der Hilfe zu Kaspersky Security Center*. Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Computer im Ereignisprotokoll von Windows und in den Berichten von Kaspersky Endpoint Security gespeichert.

Zugriffssteuerung für Aufgaben

Die Rechte für den Zugriff auf die Aufgaben von Kaspersky Endpoint Security (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Kaspersky Security Center Administrationsserver besitzt. Die Rechte werden über die Zugriffseinstellungen für die Funktionsbereiche von Kaspersky Endpoint Security zugeteilt. Um den Zugriff auf die Funktionsbereiche von Kaspersky Endpoint Security anzupassen, gehen Sie im Eigenschaftenfenster des Kaspersky Security Center-Administrationsservers zum Abschnitt **Sicherheit**. Weitere Informationen zur Konzeption der Aufgabenverwaltung über Kaspersky Security Center finden Sie *in der Hilfe zu Kaspersky Security Center*.

Die Zugriffsrechte der Benutzer für Aufgaben können Sie mithilfe der Richtlinie anpassen (*Modus für die Arbeit mit Aufgaben*). Sie können beispielsweise Gruppenaufgaben auf der Benutzeroberfläche von Kaspersky Endpoint Security ausblenden.

So konfigurieren Sie den Aufgabenverwaltungsmodus in der Benutzeroberfläche von Kaspersky Endpoint Security über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Lokale Aufgaben** → **Aufgabenverwaltung** aus.
6. Passen Sie den Modus für die Arbeit mit Aufgaben an (s. folgende Tabelle).
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Aufgabenverwaltungsmodus in der Benutzeroberfläche von Kaspersky Endpoint Security über die Web Console

1. Wählen Sie im Hauptfenster der Web Console die Registerkarte **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Unterstützung des portablen Modus aktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Lokale Aufgaben** → **Aufgabenverwaltung**.
5. Passen Sie den Modus für die Arbeit mit Aufgaben an (s. folgende Tabelle).
6. Klicken Sie auf **OK**.
7. Bestätigen Sie die Änderungen durch Klick auf **Speichern**.

Einstellungen für die Aufgabenverwaltung

Einstellung	Beschreibung
Verwendung lokaler Aufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden die lokalen Aufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Sofern die Richtlinie keine zusätzlichen Einschränkungen festlegt, kann der Benutzer Aufgaben anpassen und starten. Das Konfigurieren eines Ausführungszeitplan ist für den Benutzer jedoch weiterhin nicht verfügbar. Der Benutzer kann Aufgaben nur manuell ausführen. Ist dieses Kontrollkästchen deaktiviert, so können lokale Aufgaben nicht verwendet werden. In diesem Modus werden lokale Aufgaben nicht nach Zeitplan gestartet. Aufgaben können auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht gestartet und geändert werden. Dies gilt auch bei Verwendung der Befehlszeile. Der Benutzer kann wie bisher die Untersuchung einer Datei oder eines Ordners starten und dazu den Punkt **Auf Viren untersuchen** im Kontextmenü der Datei oder des Ordners verwenden. Dabei wird die Untersuchungsaufgabe mit den Einstellungswerten ausgeführt, die standardmäßig für die Aufgabe zur benutzerdefinierten Untersuchung gelten.
Anzeige von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden Gruppenaufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Der Benutzer kann auf der Benutzeroberfläche die komplette Aufgabenliste einsehen. Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Endpoint Security eine leere Aufgabenliste an.
Verwaltung von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer die Gruppenaufgaben starten und anhalten, die in Kaspersky Security Center festgelegt wurden. Der Benutzer kann Aufgaben auf der Benutzeroberfläche oder auf der vereinfachten Programmoberfläche starten und anhalten. Wenn das Kontrollkästchen deaktiviert ist, startet entweder Kaspersky Endpoint Security die Aufgaben automatisch nach Zeitplan oder der Administrator startet die Aufgaben manuell in Kaspersky Security Center.

Lokale Programmeinstellungen anpassen

Im Kaspersky Security Center können Sie die Einstellungen von Kaspersky Endpoint Security auf einem bestimmten Computer konfigurieren. Sie sind die *lokalen Programmeinstellungen*. Bestimmte Einstellungen können möglicherweise nicht geändert werden. Diese Einstellungen sind durch das Attribut in den Eigenschaften der Richtlinie blockiert.

So konfigurieren Sie die lokalen Programmeinstellungen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, für den Sie Kaspersky Endpoint Security anpassen möchten.
5. Wählen Sie im Kontextmenü des Client-Computers den Punkt **Eigenschaften** aus.

   Das Eigenschaftenfenster des Client-Computers wird geöffnet.
6. Wählen Sie im Eigenschaftenfenster des Client-Computers den Abschnitt **Programme**.

   Im rechten Teil des Eigenschaftenfensters des Client-Computers wird eine Liste der auf dem Client-Computer installierten Kaspersky-Programme angezeigt.
7. Wählen Sie das Programm Kaspersky Endpoint Security aus.
8. Klicken Sie unter der Liste der Kaspersky-Programme auf **Eigenschaften**.

   Das Fenster **Programmeinstellungen „Kaspersky Endpoint Security für Windows"** wird geöffnet.
9. Passen Sie im Abschnitt **Allgemeine Einstellungen** die Einstellungen von Kaspersky Endpoint Security sowie die Einstellungen für Berichte und Speicher an.

   Die übrigen Abschnitte des Fensters **Programmeinstellungen für „Kaspersky Endpoint Security für Windows"** sind identisch mit den Standardabschnitten in Kaspersky Security Center. Eine Beschreibung dieser Abschnitte finden Sie in der Hilfe zu Kaspersky Security Center.

   Wurde für das Programm eine Richtlinie erstellt, durch die eine Änderung bestimmter Einstellungen untersagt ist, so können diese Einstellungen nicht geändert werden, während die Programmeinstellungen im Abschnitt **Allgemeine Einstellungen** angepasst werden.
10. Um die vorgenommenen Änderungen zu speichern, klicken Sie im Fenster **Programmeinstellungen „Kaspersky Endpoint Security für Windows"** auf **OK**.

So konfigurieren Sie die lokalen Programmeinstellungen in der Web Console und der Cloud-Konsole

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Verwaltete Geräte** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie die Registerkarte **Programme**.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows**.

   Die lokalen Programmeinstellungen werden geöffnet.
5. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
6. Passen Sie die lokalen Programmeinstellungen an.
7. Die lokalen Programmeinstellungen entsprechen den Einstellungen der Richtlinie, unter Ausnahme der Verschlüsselungseinstellungen.

Kaspersky Endpoint Security starten und beenden

Nach der Installation von Kaspersky Endpoint Security auf dem Benutzercomputer wird das Programm automatisch gestartet. Künftig wird Kaspersky Endpoint Security standardmäßig sofort nach dem Betriebssystem gestartet. Der automatische Programmstart kann in den Einstellungen des Betriebssystems nicht angepasst werden.

Nach dem Start des Betriebssystems kann es bis zu zwei Minuten dauern, bis die Antiviren-Datenbanken für Kaspersky Endpoint Security geladen sind. Die Dauer ist von der Leistung (den technischen Möglichkeiten) des Computers abhängig. In diesem Zeitraum ist das Schutzniveau des Computers reduziert. Werden die Antiviren-Datenbanken beim Start des Programms Kaspersky Endpoint Security geladen, wenn das Betriebssystem bereits gestartet wurde, so wird das Schutzniveau des Computers dadurch nicht negativ beeinflusst.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Programmeinstellungen** aus.
6. Passen Sie mithilfe des Kontrollkästchens **Kaspersky Endpoint Security für Windows beim Hochfahren des Computers starten** den Programmstart an.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Web Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security für jene Computer, auf denen Sie den Programmstart anpassen möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Allgemeine Einstellungen** aus.
5. Klicken Sie auf den Link **Programmeinstellungen**.
6. Passen Sie mithilfe des Kontrollkästchens **Kaspersky Endpoint Security für Windows beim Hochfahren des Computers starten** den Programmstart an.
7. Klicken Sie auf **OK**.
8. Bestätigen Sie die Änderungen durch Klick auf **Speichern**.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Verwenden Sie das Kontrollkästchen **Beim Computerstart starten**, um den Start des Programms zu konfigurieren.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Die Kaspersky-Experten warnen davor, Kaspersky Endpoint Security zu beenden, da Ihr Computer und Ihre Daten dann bedroht sind. Bei Bedarf können Sie den Computerschutz für einen bestimmten Zeitraum anhalten, ohne das Programm zu beenden.

Den Programmstatus können Sie mithilfe des Widgets **Schutzstatus** überwachen.

So starten oder stoppen Sie Kaspersky Endpoint Security in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, auf dem Sie das Programm starten oder beenden möchten.
5. Öffnen Sie durch Rechtsklick das Kontextmenü des Client-Computers und wählen Sie den Punkt **Eigenschaften**.
6. Wählen Sie im Eigenschaftenfenster des Client-Computers den Abschnitt **Programme**.

   Im rechten Teil des Eigenschaftenfensters des Client-Computers wird eine Liste der auf dem Client-Computer installierten Kaspersky-Programme angezeigt.
7. Wählen Sie das Programm Kaspersky Endpoint Security aus.
8. Gehen Sie wie folgt vor:
   - Wenn Sie das Programm starten möchten, klicken Sie rechts von der Liste der Kaspersky-Programme auf die Schaltfläche  .
   - Wenn Sie das Programm beenden möchten, klicken Sie rechts von der Liste der Kaspersky-Programme auf die Schaltfläche  .

So starten oder stoppen Sie Kaspersky Endpoint Security in der Web Console

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Verwaltete Geräte** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie Kaspersky Endpoint Security starten oder beenden möchten.

   Das Eigenschaftenfenster des Computers wird geöffnet.
3. Wählen Sie die Registerkarte **Programme**.
4. Aktivieren Sie das Kontrollkästchen neben **Kaspersky Endpoint Security für Windows**.
5. Klicken Sie auf **Start** oder **Abbrechen**.

So starten oder stoppen Sie Kaspersky Endpoint Security von der Befehlszeile

Um das Programm aus der Befehlszeile zu beenden, muss die externe Steuerung von Systemdiensten aktiviert werden.

Um das Programm aus der Befehlszeile zu starten oder zu beenden, wird die Datei klpsm.exe verwendet, die zum Lieferumfang von Kaspersky Endpoint Security gehört.

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Um das Programm zu starten, geben Sie in der Befehlszeile ein: `klpsm.exe start_avp_service`.
4. Um das Programm zu beenden, geben Sie in der Befehlszeile ein: `klpsm.exe stop_avp_service`.

Anhalten und Fortsetzen von Computerschutz und -kontrolle

Werden der Schutz und die Kontrolle des Computers angehalten, so werden alle Schutzkomponenten und alle Kontrollkomponenten von Kaspersky Endpoint Security vorübergehend deaktiviert.

Der Programmstatus wird mit dem Programmsymbol im Infobereich der Taskleiste visualisiert:

- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers angehalten sind.
- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers aktiviert sind.

Wenn der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, hat dies keinen Einfluss auf die Ausführung von Untersuchungs- und Update-Aufgaben.

Wenn zum Zeitpunkt, zu dem der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, Netzwerkverbindungen bestehen, informiert eine Bildschirmmeldung darüber, dass diese Verbindungen getrennt werden.

Um den Schutz und die Kontrolle des Computers fortzusetzen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Wählen Sie im Kontextmenü **Schutz anhalten** (siehe Abbildung unten).
   Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist.
3. Wählen Sie eine der vorgeschlagenen Varianten aus:
   - **Anhalten für <Zeitraum>** – Der Schutz und die Kontrolle des Computers werden nach Ablauf des Zeitraums aktiviert, der in der Dropdown-Liste festgelegt wird.
   - **Anhalten bis zum Neustart des Programms** – Der Schutz und die Kontrolle des Computers werden nach einem Neustart des Programms oder des Betriebssystems aktiviert. Um diese Option zu verwenden, muss der automatische Programmstart aktiviert sein.
   - **Anhalten** – Der Schutz und die Kontrolle des Computers werden aktiviert, wenn Sie sie fortsetzen.

4. Klicken Sie auf die Schaltfläche **Schutz anhalten**.

Kaspersky Endpoint Security hält alle Schutz- und Kontrollkomponenten an, die in der Richtlinie kein Vorhängeschloss (🔒) haben. Bevor dieser Vorgang ausgeführt wird, sollte die Richtlinie für Kaspersky Security Center deaktiviert werden.

Kontextmenü des Programmsymbols

Gehen Sie folgendermaßen vor, um den Schutz und die Kontrolle des Computers fortzusetzen:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.

2. Wählen Sie im Kontextmenü den Punkt **Schutz fortsetzen**.

Sie können den Schutz und die Kontrolle des Computers jederzeit fortsetzen, unabhängig davon, auf welche Weise der Schutz und die Kontrolle des Computers zuvor angehalten wurden.

Untersuchung des Computers

Die Untersuchung auf Viren ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Untersuchungen auf Viren sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden.

Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, werden nicht durch Kaspersky Endpoint Security untersucht. Es werden aber Berichtseinträge darüber erstellt, dass diese Dateien nicht untersucht wurden.

Vollständige Untersuchung

Ausführliche Untersuchung des Systems. Kaspersky Endpoint Security untersucht folgende Objekte:

- Arbeitsspeicher des Kerns
- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Bootsektoren
- Backup des Betriebssystems
- alle Festplatten und Wechseldatenträger

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Vollständige Untersuchung* zu ändern.

Um Computerressourcen zu sparen, wird empfohlen, statt der Aufgabe zur vollständigen Untersuchung die Aufgabe zur Untersuchung im Hintergrund zu starten. Dabei bleibt das Niveau des Computerschutzes unverändert.

Untersuchung wichtiger Bereiche

Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Schnelle Untersuchung* zu ändern.

Benutzerdefinierte Untersuchung

Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte. Sie können ein beliebiges Objekt aus der folgenden Liste untersuchen:

- Arbeitsspeicher des Kerns

- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Backup des Betriebssystems
- Microsoft-Outlook-Postfach
- Festplatten, Wechseldatenträger und Netzlaufwerke
- Eine beliebige ausgewählte Datei

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Modus von Kaspersky Endpoint Security, in welchem dem Benutzer keine Benachrichtigungen angezeigt werden. Die Untersuchung im Hintergrund erfordert weniger Computerressourcen als andere Untersuchungstypen (z. B. vollständige Untersuchung). In diesem Modus untersucht Kaspersky Endpoint Security die Autostart-Objekte, den Bootsektor, den Systemspeicher und die Systempartition.

Integritätsprüfung

Kaspersky Endpoint Security überprüft, ob die Programm-Module Beschädigungen oder Änderungen aufweisen.

Untersuchungsaufgabe starten und abbrechen

Unabhängig vom Startmodus kann eine Untersuchungsaufgabe jederzeit gestartet oder abgebrochen werden.

Gehen Sie folgendermaßen vor, um die Untersuchungsaufgabe zu starten oder zu beenden:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wenn Sie die Untersuchungsaufgabe starten möchten, klicken Sie auf **Untersuchung starten**.

   Kaspersky Endpoint Security beginnt mit der Untersuchung des Computers. Das Programm zeigt den Untersuchungsfortschritt, die Anzahl der untersuchten Dateien und die verbleibende Untersuchungszeit an. Sie können die Aufgabe jederzeit beenden, indem Sie auf die Schaltfläche **Stopp** klicken.

Um eine Untersuchungsaufgabe von der einfachen Programmoberfläche aus zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:
   - Wählen Sie eine nicht gestartete Untersuchungsaufgabe aus, um sie zu starten.
   - Wählen Sie eine laufende Untersuchungsaufgabe aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Untersuchungsaufgabe aus, um sie erneut zu starten.

Sicherheitsstufe ändern

Kaspersky Endpoint Security kann verschiedene Gruppen von Einstellungen für die Ausführung einer Untersuchung verwenden. Diese Einstellungssätze, die im Programm gespeichert sind, heißen *Sicherheitsstufen*: **Hoch**, **Empfohlen**, **Niedrig**. Die Einstellungen der Sicherheitsstufe **Empfohlen** gelten als optimal. Sie werden von den Kaspersky-Experten angeraten. Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Um die Sicherheitsstufe zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Führen Sie unter **Sicherheitsstufe** eine der folgenden Aktionen aus:
   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:
     - **Hoch**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung von zusammengesetzten Dateien untersucht Kaspersky Endpoint Security zusätzlich Dateien in Mailformaten.
     - **Empfohlen**. Kaspersky Endpoint Security untersucht nur die Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Außerdem werden angehängte OLE-Dateien überprüft. Archive und Installationspakete werden nicht von Kaspersky Endpoint Security untersucht.
     - **Niedrig**. Kaspersky Endpoint Security untersucht nur neue und veränderte Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden nicht von Kaspersky Endpoint Security untersucht.
   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Einstellungen für die Komponenten fest.

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen, indem Sie auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen** im oberen Teil des Fensters klicken.
4. Speichern Sie die vorgenommenen Änderungen.

Aktion für infizierte Dateien ändern

Beim Fund von infizierten Dateien versucht Kaspersky Endpoint Security standardmäßig, diese Dateien zu desinfizieren oder, falls eine Desinfektion nicht möglich ist, zu löschen.

Gehen Sie folgendermaßen vor, um die Aktion für infizierte Dateien zu ändern:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** eine der folgenden Optionen aus:

- **Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht.

- **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.

- **Informieren** Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.

Bevor Sie versuchen, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt Kaspersky Endpoint Security eine Sicherungskopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

Beim Fund infizierter Dateien, die Teile einer App aus dem Windows Store sind, versucht Kaspersky Endpoint Security, die Datei zu löschen.

4. Speichern Sie die vorgenommenen Änderungen.

Liste der Untersuchungsobjekte erstellen

Um eine Liste mit Untersuchungsobjekten anzulegen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf den Link **Untersuchungsbereich bearbeiten**.
4. Wählen Sie im geöffneten Fenster die Objekte aus, die Sie dem Untersuchungsbereich hinzufügen oder von ihm ausschließen möchten.

   Objekte, die standardmäßig zum Untersuchungsbereich gehören, können nicht gelöscht oder geändert werden.

5. Um ein neues Objekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

   Der Ordnerbaum wird geöffnet.

   b. Wählen Sie ein Objekt und klicken Sie auf **Auswählen**.

   Sie können ein Objekt von Untersuchungen ausschließen, ohne es aus der Liste der Objekte im Untersuchungsbereich zu löschen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

6. Speichern Sie die vorgenommenen Änderungen.

Typ der zu untersuchenden Dateien wählen

Bei der Auswahl des Typs für die zu untersuchenden Dateien sollte Folgendes beachtet werden:

1. Für bestimmte Dateiformate (z. B. TXT-Format) besteht eine geringe Wahrscheinlichkeit, dass schädlicher Code eindringt und dann aktiviert wird. Es gibt aber auch Dateiformate, die ausführbaren Code enthalten (z. B. die Formate EXE und DLL). Ausführbarer Code kann auch in Dateiformaten enthalten sein, die dafür nicht vorgesehen sind (z. B. das Format DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist hoch.

2. Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in TXT geändert wurde, an Ihren Computer senden. Wenn Sie die Dateiuntersuchung nach Erweiterung festgelegt haben, überspringt das Programm eine solche Datei bei der Untersuchung. Wenn die Überprüfung von Dateien nach Format ausgewählt wird, analysiert Kaspersky Endpoint Security den Datei-Header unabhängig von seiner Erweiterung. Falls sich ergibt, dass die Datei das Format einer ausführbaren Datei (beispielsweise EXE) besitzt, so wird die Datei untersucht.

Um einen Typ für die zu untersuchenden Dateien auszuwählen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.

2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Geben Sie unter **Dateitypen** den Typ der Dateien an, die von der gewählten Untersuchungsaufgabe untersucht werden sollen:

   - **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung).

   - **Dateien nach Format untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht.

   - **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.

   Dateien ohne Erweiterung werden von Kaspersky Endpoint Security als ausführbar betrachtet. Ausführbare Dateien werden immer von Kaspersky Endpoint Security untersucht, unabhängig davon, welchen Dateityp Sie für die Untersuchung gewählt haben.

5. Speichern Sie die vorgenommenen Änderungen.

Dateiuntersuchung optimieren

Die Dateiuntersuchung lässt sich in folgender Hinsicht optimieren: Untersuchungsdauer verkürzen und Arbeitsgeschwindigkeit von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien. Außerdem können Sie die Untersuchungsdauer für eine einzelne Datei beschränken. Nach Ablauf des vorgegebenen Zeitraums schließt Kaspersky Endpoint Security eine Datei aus der laufenden Untersuchung aus (außer Archiven und Objekten, die aus mehreren Dateien bestehen).

Außerdem können Sie Verwendung der Technologien iChecker und iSwift aktivieren. Mit den Technologien iChecker und iSwift lässt sich die Dateiuntersuchung beschleunigen. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Untersuchung von Dateien zu optimieren:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie im Block **Untersuchung optimieren** die Untersuchungseinstellungen:
   - **Nur neue und veränderte Dateien untersuchen**. Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.
   - **Dateien überspringen, wenn Untersuchung länger dauert als n Sek**. Beschränkt die Untersuchungsdauer für ein einzelnes Objekt. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Dateiuntersuchung ab. Dadurch lässt sich die Untersuchungsdauer reduzieren.
5. Speichern Sie die vorgenommenen Änderungen.

Untersuchung von zusammengesetzten Dateien

Eine häufig anzutreffende Methode zum Verstecken von Viren und anderen gefährlichen Programmen ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive oder Datenbanken. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Installationspakete, Office-Format-Dateien, in Mail-Format-Dateien, kennwortgeschützte Archive.

5. Wenn die Untersuchung nur neuer und geänderter Dateien deaktiviert ist, konfigurieren Sie die Einstellungen für die Untersuchung jedes Typs von zusammengesetzten Dateien: „Alle Dateien dieses Typs untersuchen“ oder „Nur neue Dateien untersuchen“.

   Wenn die Untersuchung nur neuer und geänderter Dateien aktiviert ist, überprüft Kaspersky Endpoint Security nur neue und geänderte Dateien aller Arten von zusammengesetzten Dateien.

6. Führen Sie unter **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße** einen entsprechenden Wert an, wenn umfangreiche zusammengesetzte Dateien nicht entpackt werden sollen.

   - Damit zusammengesetzte Dateien unabhängig von ihrer Größe entpackt werden, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

7. Speichern Sie die vorgenommenen Änderungen.

Untersuchungsmethoden verwenden

Kaspersky Endpoint Security verwendet die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse. Bei der Signaturanalyse vergleicht Kaspersky Endpoint Security ein gefundenes Objekt mit den Einträgen in den Programm-Datenbanken. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.

Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.

Gehen Sie folgendermaßen vor, um die Untersuchungsmethoden zu verwenden:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.

2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wenn Sie möchten, dass das Programm die heuristische Analyse beim Ausführen der Untersuchungsaufgabe verwendet, aktivieren Sie das Kontrollkästchen **Heuristische Analyse** im Block **Untersuchungsmethoden**. Legen Sie dann mit dem Schieberegler die Stufe der heuristischen Analyse fest: **oberflächlich**, **mittel** oder **tief**.

5. Speichern Sie die vorgenommenen Änderungen.

Untersuchungstechnologien verwenden

Gehen Sie folgendermaßen vor, um die Untersuchungstechnologien zu verwenden:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

   - **iSwift-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - **iChecker-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

5. Speichern Sie die vorgenommenen Änderungen.

Startmodus für eine Untersuchungsaufgabe wählen

Ist der Start der Untersuchungsaufgabe nicht möglich (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass der Start einer übersprungenen Untersuchungsaufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Sie können den Start der Untersuchungsaufgabe nach dem Programmstart aufschieben, wenn die Startzeit der Untersuchungsaufgabe mit der Startzeit von Kaspersky Endpoint Security übereinstimmt. Die Untersuchungsaufgabe wird erst dann gestartet, wenn der vorgegebene Zeitraum nach dem Start von Kaspersky Endpoint Security verstrichen ist.

Um einen Startmodus für die Untersuchungsaufgabe zu wählen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf die Schaltfläche **Untersuchungszeitplan**.
4. Konfigurieren Sie im geöffneten Fenster den Zeitplan für die Ausführung der Untersuchungsaufgabe.
5. Passen Sie je nach gewählter Frequenz die erweiterten Einstellungen für den Startzeitplan der Aufgabe an.

   a. Aktivieren Sie das Kontrollkästchen **Geplante Untersuchung am nächsten Tag starten, falls der Computer ausgeschaltet ist**, damit Kaspersky Endpoint Security übersprungene Untersuchungsaufgaben bei der

nächsten Gelegenheit ausführt.

> Ist das Element **Jede Minute**, **Stündlich**, **Nach Programmstart** oder **Nach jedem Update** in der Dropdown-Liste **Untersuchung durchführen** ausgewählt, so ist das Kontrollkästchen **Geplante Untersuchung am nächsten Tag starten, falls der Computer ausgeschaltet ist** nicht verfügbar.

b. Aktivieren Sie das Kontrollkästchen **Nur ausführen, wenn der Computer inaktiv ist**, damit Kaspersky Endpoint Security die Aufgabe anhält, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist.

   Diese Zeitplanvariante erlaubt einen sparsamen Umgang mit der Rechnerleistung.

6. Speichern Sie die vorgenommenen Änderungen.

Start der Untersuchungsaufgabe mit den Rechten eines anderen Benutzers anpassen

Die Untersuchungsaufgabe wird standardmäßig mit den Rechten des Benutzerkontos gestartet, mit welchem der Benutzer im Betriebssystem angemeldet ist. Es kann aber erforderlich sein, eine Untersuchungsaufgabe mit den Rechten eines anderen Benutzers zu starten. Sie können in den Einstellungen der Untersuchungsaufgabe einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Untersuchungsaufgabe im Namen dieses Benutzers starten.

Gehen Sie folgendermaßen vor, um den Start der Untersuchungsaufgabe mit den Rechten eines anderen Benutzers zu konfigurieren:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Klicken Sie auf **Erweiterte Einstellungen** → **Untersuchung ausführen als**.
4. Wählen Sie im geöffneten Fenster den Benutzer aus, der die Rechte zum Starten der Untersuchungsaufgabe benötigt.
5. Speichern Sie die vorgenommenen Änderungen.

Wechseldatenträger beim Anschließen an den Computer untersuchen

Kaspersky Endpoint Security untersucht alle Dateien, die Sie ausführen oder kopieren, selbst wenn die sich die Datei auf einem Wechseldatenträger befindet (Komponente „Schutz vor bedrohlichen Dateien“). Um die Ausbreitung von Viren und anderer Schadsoftware zu verhindern, können Sie festlegen, dass Wechseldatenträger automatisch untersucht werden, wenn sie mit dem Computer verbunden werden. Kaspersky Endpoint Security versucht automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. Die Komponente sorgt für die Sicherheit eines Computers und nutzt dafür Untersuchungen, die maschinelles Lernen, heuristische Analyse (hohe Ebene) und Signaturanalyse implementieren. Außerdem verwendet Kaspersky Endpoint Security zur Untersuchungsoptimierung die Technologien iSwift und iChecker. Diese Technologien sind immer aktiviert und können nicht deaktiviert werden.

Um die Untersuchung von Wechseldatenträgern anzupassen, wenn diese mit dem Computer verbunden werden, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe „Wechseldatenträger“ und klicken Sie auf die Schaltfläche ⚙.
3. Verwenden Sie den Schalter für die **Untersuchung von Wechseldatenträgern**, um die Untersuchung von Wechseldatenträgern beim Anschließen an den Computer zu aktivieren oder zu deaktivieren.
4. Wählen Sie den Modus zum Untersuchen von Wechseldatenträgern beim Anschließen:
   - **Detaillierte Untersuchung** Ist diese Variante ausgewählt, so untersucht Kaspersky Endpoint Security nach dem Anschließen eines Wechseldatenträgers alle Dateien, die sich auf dem Wechseldatenträger befinden, einschließlich Dateien, die in zusammengesetzte Objekte, Archive, Programmpakete und Office-Format-Dateien eingebettet sind. Kaspersky Endpoint Security untersucht Dateien in Mail-Formaten und kennwortgeschützte Archive nicht.
   - **Schnelle Untersuchung** Ist diese Variante ausgewählt, so untersucht Kaspersky Endpoint Security nach dem Anschließen eines Wechseldatenträgers nur Dateien mit bestimmten Formaten, die als besonders infektionsanfällig gelten. Außerdem werden zusammengesetzte Objekte nicht entpackt.
5. Damit Kaspersky Endpoint Security nur Wechseldatenträger untersucht, deren Größe den festgelegten Wert nicht überschreitet, aktivieren Sie das Kontrollkästchen **Maximale Größe des Wechseldatenträgers** und geben Sie im nebenstehenden Feld einen Wert in Megabyte an.
6. Passen Sie an, wie der Untersuchungsfortschritt für einen Wechseldatenträger angezeigt werden soll. Führen Sie eine der folgenden Aktionen aus:
   - Damit das Programm Kaspersky Endpoint Security den Fortschritt der Untersuchung von Wechseldatenträgern in einem separaten Fenster anzeigt, aktivieren Sie das Kontrollkästchen **Untersuchungsfortschritt anzeigen**.

     Der Benutzer kann die Untersuchung im Fenster der Wechseldatenträger-Untersuchung beenden. Um die obligatorische Untersuchung von Wechseldatenträgern festzulegen und dem Benutzer zu verbieten, die Untersuchung abzubrechen, aktivieren Sie das Kontrollkästchen **Beenden der Untersuchungsaufgabe verbieten**.
   - Damit das Programm Kaspersky Endpoint Security die Untersuchung von Wechseldatenträgern im Hintergrundmodus ausführt, deaktivieren Sie das Kontrollkästchen **Untersuchungsfortschritt anzeigen**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Modus von Kaspersky Endpoint Security, in welchem dem Benutzer keine Benachrichtigungen angezeigt werden. Die Untersuchung im Hintergrund erfordert weniger Computerressourcen als andere Untersuchungstypen (z. B. vollständige Untersuchung). In diesem Modus untersucht Kaspersky Endpoint Security die Autostart-Objekte, den Bootsektor, den Systemspeicher und die Systempartition. Die Untersuchung im Hintergrund wird in folgenden Fällen gestartet:

- nach dem Update der Antiviren-Datenbanken
- 30 Minuten nach dem Start von Kaspersky Endpoint Security

- alle sechs Stunden
- Wenn der Computer für fünf Minuten oder länger im Leerlauf ist (der Computer ist gesperrt oder der Bildschirmschoner ist eingeschaltet).

Die Hintergrunduntersuchung bei Inaktivität des Computers wird unterbrochen, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Computer hat in den aktiven Modus gewechselt.

  Wenn die Untersuchung im Hintergrund seit über zehn Tagen nicht mehr ausgeführt wurde, wird die Untersuchung nicht unterbrochen.

- Der Computer (das Notebook) hat in den Batteriebetrieb gewechselt.

Wenn die Aufgabe „Hintergrunduntersuchung“ ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.

Um die Untersuchung des Computers im Hintergrund zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Aufgaben**.
2. Wählen Sie im geöffneten Fenster die Untersuchungsaufgabe und klicken Sie auf die Schaltfläche ⚙.
3. Verwenden Sie den Schalter **Untersuchung im Hintergrund**, um die Untersuchung im Hintergrund zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Integritätsprüfung für das Programm

Kaspersky Endpoint Security überprüft, ob die Programmdateien, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Beispiel: Besitzt eine Programmbibliothek eine inkorrekte digitale Signatur, so gilt diese Bibliothek als beschädigt. Zur Untersuchung von Programmdateien dient die Aufgabe *Integritätsprüfung*. Starten Sie die Aufgabe *Integritätsprüfung*, wenn das Programm Kaspersky Endpoint Security ein schädliches Objekt gefunden hat, dieses aber nicht neutralisiert wurde.

Die Aufgabe *Integritätsprüfung* können Sie in Kaspersky Security Center 12 Web Console und in der „Verwaltungskonsole“ erstellen. Diese Aufgabe kann nicht im Programm Kaspersky Security Center Cloud Console erstellt werden.

[So führen Sie eine Integritätsprüfung des Programms über die Verwaltungskonsole (MMC) durch]

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver → Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie den Punkt **Kaspersky Endpoint Security für Windows (11.6.0) → Integritätsprüfung** aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder beim Erkennen eines Virenangriffs.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen an, beispielsweise `Integritätsprüfung für das Programm nach einer Computerinfektion`.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch führt Kaspersky Endpoint Security eine Integritätsprüfung des Programms aus. Außerdem können Sie in den Aufgabeneigenschaften einen Zeitplan für die Integritätsprüfung des Programms festlegen.

[So führen Sie eine Integritätsprüfung eines Programms über die Web Console durch]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Integritätsprüfung** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Integritätsprüfung des Programms nach einer Computerinfektion`.

   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Fertig**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

Dadurch führt Kaspersky Endpoint Security eine Integritätsprüfung des Programms aus. Außerdem können Sie in den Aufgabeneigenschaften einen Zeitplan für die Integritätsprüfung des Programms festlegen.

Verletzungen der Programm-Integrität können beispielsweise in den folgenden Fällen auftreten:

- Ein schädliches Objekt hat die Dateien von Kaspersky Endpoint Security verändert. In diesem Fall führen Sie den Vorgang zur Wiederherstellung von Kaspersky Endpoint Security mit Betriebssystemmitteln aus. Starten Sie nach der Wiederherstellung eine vollständige Untersuchung des Computers und wiederholen Sie die Integritätsprüfung.
- Die digitale Signatur ist abgelaufen. In diesem Fall aktualisieren Sie Kaspersky Endpoint Security.

Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Als primäre Update-Quelle für Kaspersky Endpoint Security dienen die Update-Server von Kaspersky.

Der Computer muss mit dem Internet verbunden sein, um das Update-Paket erfolgreich von den Kaspersky-Update-Servern herunterzuladen. Standardmäßig wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, müssen Sie die Proxyserver-Einstellungen konfigurieren.

Updates werden mit dem HTTPS-Protokoll heruntergeladen. Falls ein Download mit dem HTTPS-Protokoll nicht möglich ist, erfolgt der Download mit dem HTTP-Protokoll.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Endpoint Security. Der Computerschutz basiert auf Datenbanken, die Signaturen für Viren und andere bedrohliche Programme, sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und der Desinfektion von infizierten Dateien auf dem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Endpoint Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Neben den Datenbanken von Kaspersky Endpoint Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Endpoint Security, fügen neue Funktionen hinzu und optimieren vorhandene Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Update-Quelle vorliegt. Sind die Datenbanken und Programm-Module nicht aktuell, werden fehlende Teile der Updates auf dem Computer installiert.

Beim Update der Programm-Module kann auch die Kontexthilfe für das Programm aktualisiert werden.

Sind die Datenbanken stark veraltet, kann das Update-Paket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Informationen über den aktuellen Status der Datenbanken für Kaspersky Endpoint Security werden im Block **Update** im Fenster **Aufgaben** angezeigt.

Informationen über die Aktualisierungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Update-Aufgabe auftreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Schemata für das Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Auf den Benutzercomputern werden die folgenden Objekte aktualisiert:

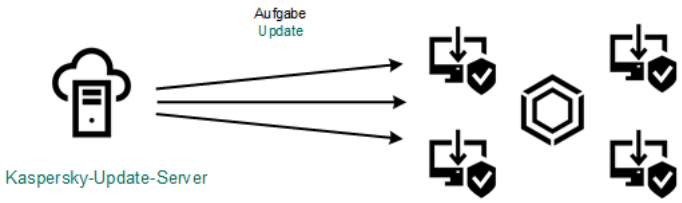
- Antiviren-Datenbanken. Die Antiviren-Datenbanken enthalten Datenbanken mit den Signaturen schädlicher Programme, Definitionen von Netzwerkangriffen, Datenbanken für bösartige Webadressen und Phishing-Webadressen, Datenbanken für Banner, Spam-Datenbanken sowie andere Daten.

- Programm-Module. Ein Update für Module dient dazu, Schwachstellen im Programm zu beheben und die Methoden des Computerschutzes zu verbessern. Bei Modul-Updates kann das Verhalten von Programmkomponenten geändert und neue Funktionen können hinzugefügt werden.

Kaspersky Endpoint Security unterstützt folgende Schemata für das Update der Datenbanken und Programm-Module:

- Update von den Kaspersky-Servern.

  Die Kaspersky-Update-Server befinden sich in unterschiedlichen Ländern. Dadurch wird die Zuverlässigkeit des Updates erhöht. Wenn das Update nicht vom einem Server ausgeführt werden kann, wechselt Kaspersky Endpoint Security zum nächsten Server.



Update von den Kaspersky-Servern.

- Zentralisiertes Update.

  Das zentralisierte Update gewährleistet eine Reduzierung des externen Internet-Datenverkehrs und eine bequeme Kontrolle des Updates.

  Das zentralisierte Update umfasst die folgenden Schritte:

  1. Upload des Update-Pakets in eine Ablage innerhalb des Unternehmensnetzwerks.

     Das Update-Paket wird mithilfe der Administrationsserver-Aufgabe *Upload von Updates in den Speicher des Administrationsservers* in eine Ablage hochgeladen.

  2. Upload des Update-Pakets in einen gemeinsamen Ordner (optional).

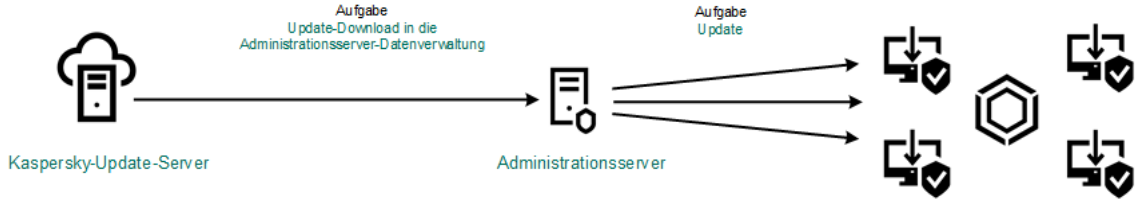
     Für den Upload des Update-Pakets in einen gemeinsamen Ordner bestehen die folgenden Möglichkeiten:

     - Mithilfe der *Update*-Aufgabe von Kaspersky Endpoint Security. Diese Aufgabe ist für einen der Computer des lokalen Unternehmensnetzwerks vorgesehen.

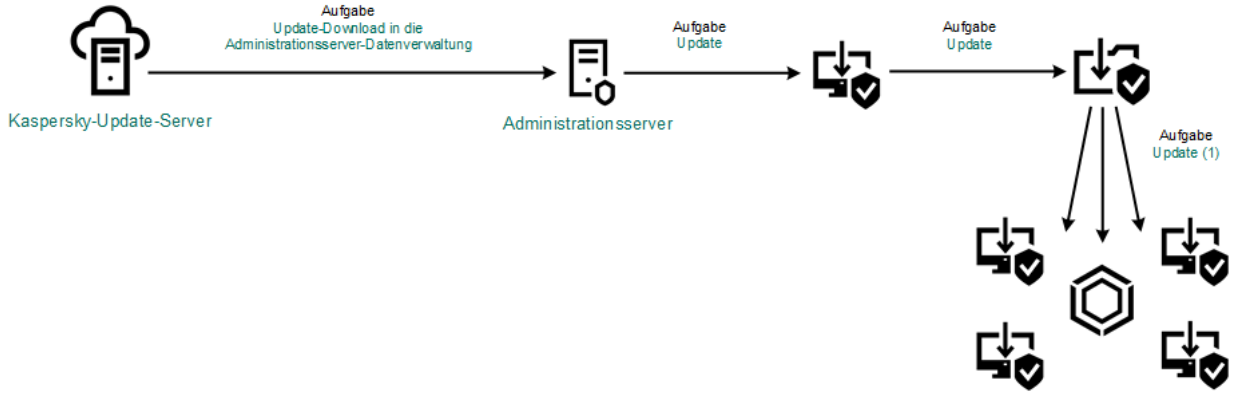
     - Mithilfe von Kaspersky Update Utility. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie *in der Wissensdatenbank von Kaspersky*.

  3. Verteilung des Update-Pakets an die Client-Computer.

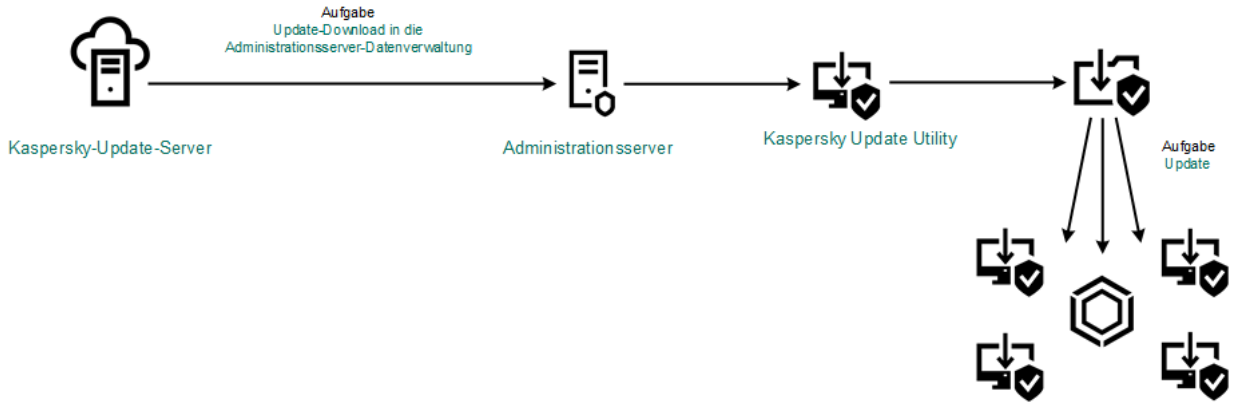
Die Verteilung des Update-Pakets an die Client-Computer wird durch die Aufgabe von Kaspersky Endpoint Security *Update* gewährleistet. Sie können eine unbeschränkte Anzahl von Update-Aufgaben für jede der Administrationsgruppen erstellen.



Update aus dem Serverspeicher



Update aus dem gemeinsamen Ordner



Update mithilfe von Kaspersky Update Utility

Für Web Console enthält die Liste der Update-Quellen standardmäßig den Administrationsserver für Kaspersky Security Center und die Kaspersky-Update-Server. Für Kaspersky Security Center Cloud Console enthält die Liste der Update-Quellen standardmäßig die Verteilungspunkte und die Kaspersky-Update-Server. Details über die Verteilungspunkte finden Sie in der *Hilfe zu Kaspersky Security Center Cloud Console*. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden. Wenn das Update von einer Update-Quelle nicht ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten.

Updates werden mit den standardmäßigen Netzwerkprotokolle von den Kaspersky-Update-Servern oder von anderen FTP- oder HTTP-Servern heruntergeladen. Wenn für den Zugriff auf eine Update-Quelle die Verbindung mit einem Proxyserver erforderlich ist, geben Sie die Proxyserver-Einstellungen in den Eigenschaften der Richtlinie für Kaspersky Endpoint Security ein.

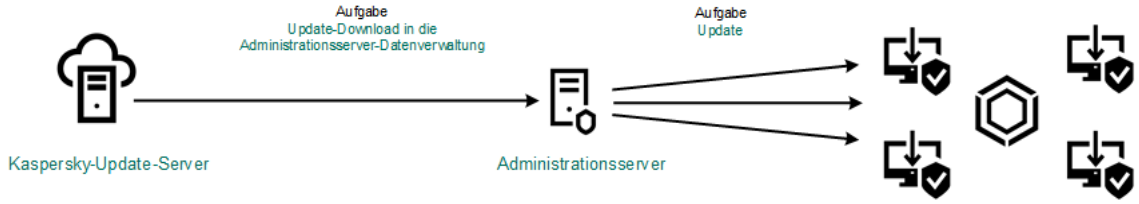
Update aus dem Serverspeicher

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update der Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus dem Serverspeicher erfolgen soll. Dabei lädt Kaspersky Security Center das Update-Paket von den Kaspersky-Update-Servern in einen Speicher (FTP-, HTTP-Server, Netzwerkordner oder lokaler Ordner) herunter. Die übrigen Computer des lokalen Unternehmensnetzwerks können das Update-Paket dann aus dem Serverspeicher abrufen.

Um das Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten, sind folgende Schritte erforderlich:

1. Anpassen des Verschiebens des Update-Pakets in einen Speicher auf dem Administrationsserver (Aufgabe *Herunterladen von Updates in die Datenverwaltung des Administrationsservers*).

2. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten Serverspeicher für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks (Aufgabe *Update*).



Update aus dem Serverspeicher

Um den Download des Update-Pakets in den Serverspeicher anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Administrationsserver-Aufgabe **Herunterladen von Updates in den Speicher des Administrationsservers**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Herunterladen von Updates in die Datenverwaltung des Administrationsservers* wird vom Schnellstartassistenten für Kaspersky Security Center 12 Web Console automatisch erstellt und kann nur in einem Exemplar vorhanden sein.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Klicken Sie im Block **Sonstige Einstellungen** auf **Anpassen**.

5. Geben Sie im Feld **Ordner für Updates** die Adresse des FTP- oder HTTP-Servers, Netzwerkordners oder lokalen Ordners an, in den Kaspersky Security Center ein Update-Paket kopieren soll, das von den Kaspersky-Update-Servern heruntergeladen wurde.

   Das Format für den Pfad einer Update-Quelle sieht wie folgt aus:

   - Geben Sie für einen FTP- oder HTTP-Server die Webadresse oder die IP-Adresse der Website ein.

     Beispielsweise `http://dnl-01.geo.kaspersky.com/` oder `93.191.13.103`.

     Für einen FTP-Server ist die Angabe der Anmeldeparameter in folgendem Format möglich: `ftp://<Benutzername>:<Kennwort>@<Knoten>:<Port>`.

   - Geben Sie für einen Netzwerkordner den UNC-Pfad ein.

Beispiel: `\\Server\Share\Update distribution`.

- Geben Sie für einen lokalen Ordner den vollständigen Ordnerpfad ein.

  Zum Beispiel, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Speichern Sie die vorgenommenen Änderungen.

Um das Update für Kaspersky Endpoint Security aus dem angegebenen Speicher des Servers anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Aufgabe von Kaspersky Endpoint Security **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird vom Schnellstartassistenten für Kaspersky Security Center automatisch erstellt. Um die Aufgabe *Updates* zu erstellen, installieren Sie mithilfe des Assistenten das Web-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Programmeinstellungen** → **Lokaler Modus** aus.

4. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

5. Geben Sie im Feld **Quelle** die Adresse des FTP- oder HTTP-Servers, Netzwerkordners oder lokalen Ordners an, in den Kaspersky Security Center ein Update-Paket kopieren soll, das von den Kaspersky-Update-Servern heruntergeladen wurde.

   Die Adresse der Quelle muss mit der Adresse übereinstimmen, die zuvor im Feld **Ordner für Updates** angegeben wurde, als der Update-Download in den Serverspeicher angepasst wurde (s. *Anleitung oben*).

6. Wählen Sie im Block **Status** die Variante **Aktiviert** aus.

7. Klicken Sie auf **OK**.

8. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

9. Klicken Sie auf **Speichern**.

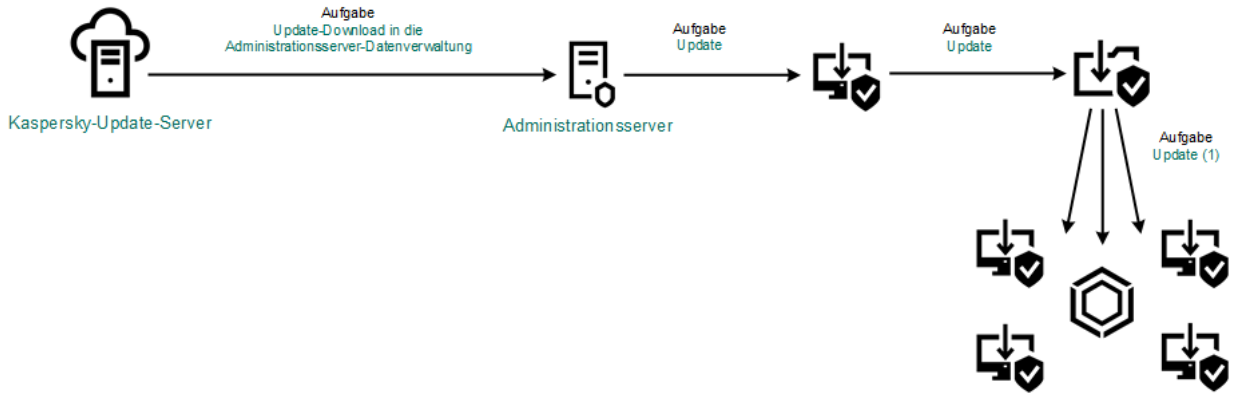
Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

Update aus dem gemeinsamen Ordner

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update der Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus einem gemeinsamen Ordner erfolgen soll. Dazu lädt ein Computer des lokalen Unternehmensnetzwerks die Update-Pakete vom Administrationsserver für Kaspersky Security Center oder von den Kaspersky-Update-Servern herunter und kopiert das heruntergeladene Update-Paket in einen gemeinsamen Ordner. In diesem Fall können die übrigen Computer des lokalen Unternehmensnetzwerks das Update-Paket aus dem gemeinsamen Ordner abrufen.

Um das Update der Datenbanken und Programm-Module aus einem gemeinsamen Ordner einzurichten, sind folgende Schritte erforderlich:

1. Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten.
2. Aktivieren Sie das Kopieren eines Update-Pakets in einen freigegebenen Ordner auf einem der Computer im Unternehmens-LAN (siehe nachstehende Anweisungen).
3. Konfigurieren Sie Datenbank- und Programm-Modul-Updates aus dem angegebenen gemeinsamen Ordner auf die übrigen Computer im Unternehmens-LAN (siehe nachstehende Anweisungen).



Update aus dem gemeinsamen Ordner

Gehen Sie folgendermaßen vor, um den Modus zur Verteilung des Update-Pakets aus einem gemeinsamen Ordner zu aktivieren:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Aufgabe von Kaspersky Endpoint Security **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird vom Schnellstartassistenten für Kaspersky Security Center automatisch erstellt. Um die Aufgabe *Updates* zu erstellen, installieren Sie mithilfe des Assistenten das Web-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Programmeinstellungen** → **Lokaler Modus** aus.

4. Passen Sie die Update-Quellen an.

   Als Update-Quellen können die Kaspersky-Update-Server, der Administrationsserver für Kaspersky Security Center oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.

5. Aktivieren Sie das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

6. Geben Sie im Feld **Pfad** den UNC-Pfad des gemeinsamen Ordners an (Beispiel: `\\Server\Share\Update distribution`).

   Wenn das Feld leer bleibt, kopiert Kaspersky Endpoint Security das Update-Paket in den Ordner `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

7. Klicken Sie auf **Speichern**.

Die Aufgabe *Update* muss einem bestimmten Computer zugewiesen werden, der als Update-Quelle dienen soll.

Um das Update aus einem gemeinsamen Ordner anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Update** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Update aus dem gemeinsamen Ordner`.

   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

   Die Aufgabe *Update* muss den übrigen Computern des lokalen Unternehmensnetzwerks zugewiesen werden, unter Ausnahme des Computers, der als Update-Quelle dient.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei, welche Variante für den Gültigkeitsbereich der Aufgabe ausgewählt wurde. Klicken Sie dann auf **Weiter**.

5. Beenden Sie den Assistenten durch Klick auf **Erstellen**.

   Die neue Aufgabe wird in der Aufgabentabelle angezeigt.

6. Klicken Sie auf die erstellte Aufgabe *Update*.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wechseln Sie zum Abschnitt **Programmeinstellungen**.

8. Wählen Sie die Registerkarte **Lokaler Modus**.

9. Klicken Sie im Block **Update-Quelle** auf **Hinzufügen**.

10. Geben Sie im Feld **Quelle** den Pfad des gemeinsamen Ordners an.

    Die Adresse der Quelle muss mit der Adresse übereinstimmen, die zuvor im Feld **Pfad** angegeben wurde, als das Kopieren des Update-Pakets in einen gemeinsamen Ordner angepasst wurde (s. *Anleitung oben*).

11. Klicken Sie auf **OK**.

12. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

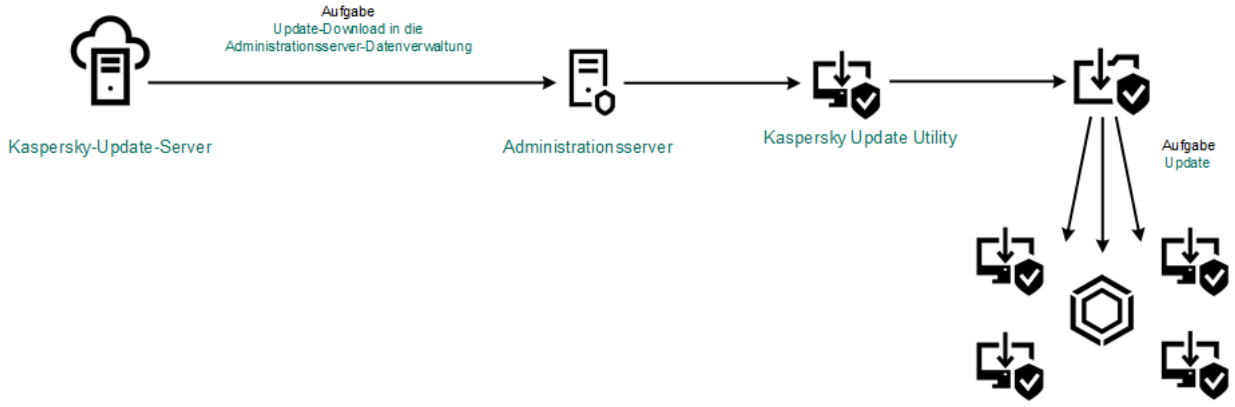
13. Klicken Sie auf **Speichern**.

Update mithilfe von Kaspersky Update Utility

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update für Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus einem gemeinsamen Ordner mithilfe des Hilfsprogramms Kaspersky Update Utility erfolgen soll. Dazu lädt ein Computer des lokalen Unternehmensnetzwerks die Update-Pakete vom Administrationsserver für Kaspersky Security Center oder von den Kaspersky-Update-Servern herunter und kopiert die heruntergeladenen Update-Pakete mithilfe des Hilfsprogramms in einen gemeinsamen Ordner. In diesem Fall können die übrigen Computer des lokalen Unternehmensnetzwerks das Update-Paket aus dem gemeinsamen Ordner abrufen.

Um das Update der Datenbanken und Programm-Module aus einem gemeinsamen Ordner einzurichten, sind folgende Schritte erforderlich:

1. Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten.
2. Installation von Kaspersky Update Utility auf einem der Computer des lokalen Unternehmensnetzwerks.
3. Kopieren des Update-Pakets in einen gemeinsamen Ordner anpassen in den Einstellungen von Kaspersky Update Utility.
4. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten gemeinsamen Ordner für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks.



Update mithilfe von Kaspersky Update Utility

Kaspersky Update Utility kann von der Website des Technischen Supports von Kaspersky heruntergeladen werden. Wählen Sie nach der Installation des Hilfsprogramms eine Update-Quelle aus (z. B. die Datenverwaltung des Administrationsservers) und einen gemeinsamen Ordner, in den Kaspersky Update Utility die Update-Pakete kopieren soll. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie *in der Wissensdatenbank von Kaspersky*.

Um das Update aus einem gemeinsamen Ordner anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Aufgabe von Kaspersky Endpoint Security **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

Die Aufgabe *Update* wird vom Schnellstartassistenten für Kaspersky Security Center automatisch erstellt. Um die Aufgabe *Updates* zu erstellen, installieren Sie mithilfe des Assistenten das Web-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Programmeinstellungen** → **Lokaler Modus** aus.
4. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.
5. Geben Sie im Feld **Quelle** den UNC-Pfad des gemeinsamen Ordners an (Beispiel: `\\Server\Share\Update distribution`).

   Die Adresse der Quelle muss mit der Adresse übereinstimmen, die in den Einstellungen von Kaspersky Update Utility angegeben ist.

6. Klicken Sie auf **OK**.
7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.
8. Klicken Sie auf **Speichern**.

Update im mobilen Modus

Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*). Details über die Verwendung von Offline-Computern und Offline-Benutzern *finden Sie in der Hilfe für Kaspersky Security Center*.

Mobile Computer außerhalb des Unternehmensnetzwerks besitzen keine Verbindung zum Administrationsserver, um die Datenbanken und Programm-Module zu aktualisieren. Im mobilen Modus werden für das Update der Datenbanken und Programm-Module standardmäßig nur die Kaspersky-Update-Server als Update-Quelle verwendet. Die Verwendung eines Proxyservers für die Internetverbindung wird durch eine spezielle mobile Richtlinie festgelegt. Die mobile Richtlinie muss separat erstellt werden. Nachdem Kaspersky Endpoint Security in den mobilen Modus gewechselt hat, wird die Update-Aufgabe alle zwei Stunden gestartet.

Um die Einstellungen für das Update im mobilen Modus anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Aufgabe von Kaspersky Endpoint Security **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird vom Schnellstartassistenten für Kaspersky Security Center automatisch erstellt. Um die Aufgabe *Updates* zu erstellen, installieren Sie mithilfe des Assistenten das Web-Plug-in für Kaspersky Endpoint Security für Windows.

   Wählen Sie die Registerkarte **Programmeinstellungen** → **Mobiler Modus** aus.

3. Passen Sie die Update-Quellen an. Als Update-Quellen können die Kaspersky-Update-Server oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.
4. Klicken Sie auf **Speichern**.

Dadurch werden die Datenbanken und Programm-Module auf den Benutzercomputern bei einem Wechsel in den mobilen Modus aktualisiert.

Update-Aufgabe starten und abbrechen

Eine Update-Aufgabe für Kaspersky Endpoint Security kann unabhängig vom gewählten Startmodus für die Update-Aufgabe jederzeit gestartet oder abgebrochen werden.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe zu starten oder zu beenden:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.
2. Klicken Sie im Block **Aktualisierung von Datenbanken und Programm-Modulen** auf die Schaltfläche **Aktualisieren**, wenn Sie die Update-Aufgabe starten möchten.

   Kaspersky Endpoint Security wird mit dem Update der Programm-Module und Datenbanken beginnen. Das Programm zeigt den Aufgabenfortschritt, die Größe der heruntergeladenen Dateien und die Update-Quelle an. Sie können jederzeit auf die Schaltfläche  klicken, um diese Aufgabe zu beenden.

Um von der einfachen Programmoberfläche aus eine Update-Aufgabe zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:
   - Wählen Sie eine nicht gestartete Update-Aufgabe aus, um sie zu starten.
   - Wählen Sie eine laufende Update-Aufgabe aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Update-Aufgabe aus, um sie erneut zu starten.

Update-Aufgabe mit den Rechten eines anderen Benutzers starten

Die Update-Aufgabe für Kaspersky Endpoint Security wird standardmäßig im Namen des Benutzers gestartet, mit dessen Rechten Sie sich im Betriebssystem angemeldet haben. Das Update für Kaspersky Endpoint Security kann aber auch aus einer Update-Quelle erfolgen, für welche der Benutzer keine Zugriffsrechte besitzt (z. B. aus einem gemeinsamen Ordner, welcher das Update-Paket enthält) oder für welche die Verwendung der Authentifizierung auf dem Proxyserver nicht angepasst ist. Sie können in den Einstellungen für Kaspersky Endpoint Security einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Update-Aufgabe für Kaspersky Endpoint Security im Namen dieses Benutzers starten.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe mit den Rechten eines anderen Benutzers zu starten:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.
2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.
3. Klicken Sie auf die Schaltfläche **Benutzerkonto-Einstellungen**.

4. Wählen Sie im geöffneten Fenster die Option **Datenbanken-Update mit Benutzerrechten ausführen**.

5. Geben Sie die Konto-Anmeldedaten eines Benutzers mit den erforderlichen Berechtigungen für den Zugriff auf die Update-Quelle ein.

6. Speichern Sie die vorgenommenen Änderungen.

Startmodus für die Update-Aufgabe wählen

Ist der Start der Update-Aufgabe nicht möglich (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass der Start einer übersprungenen Update-Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Sie können festlegen, dass der Start der Update-Aufgabe nach dem Start des Programms aufgeschoben wird. Dies ist möglich, wenn Sie für die Update-Aufgabe den Startmodus **Nach Zeitplan** gewählt haben und der Startzeitpunkt von Kaspersky Endpoint Security mit dem Startzeitplan der Update-Aufgabe übereinstimmt. Die Update-Aufgabe wird erst dann gestartet, wenn der vorgegebene Zeitraum nach dem Start von Kaspersky Endpoint Security verstrichen ist.

Um einen Startmodus für die Update-Aufgabe zu wählen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.

2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.

3. Klicken Sie auf die Schaltfläche **Datenbanken-Update-Modus einstellen**.

4. Wählen Sie im geöffneten Fenster den Ausführungsmodus der Update-Aufgabe:

   - Wählen Sie die Option **Automatisch**, damit Kaspersky Endpoint Security beim Start der Update-Aufgabe berücksichtigt, ob an der Update-Quelle ein Update-Paket vorhanden ist. Die Häufigkeit, mit der Kaspersky Endpoint Security nach einem neuen Update-Paket sucht, kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken.

   - Wählen Sie die Option **Manuell**, wenn Sie die Update-Aufgabe manuell starten möchten.

   - Wählen Sie die Option <**Nach Zeitplan**>, um einen Startzeitplan für die Update-Aufgabe anzupassen. Konfigurieren Sie die erweiterten Einstellungen für den Start der Update-Aufgabe:

     - Geben Sie im Feld **Ausführung nach Programmstart aufschieben für** an, für welchen Zeitraum der Start der Update-Aufgabe nach dem Start von Kaspersky Endpoint Security aufgeschoben werden soll.

     - Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, damit Kaspersky Endpoint Security Update-Aufgaben, die nicht rechtzeitig gestartet werden konnten, so bald wie möglich ausführt.

5. Speichern Sie die vorgenommenen Änderungen.

Update-Quelle hinzufügen

Eine *Update-Quelle* ist eine Ressource, die Updates der Datenbanken und der Programm-Module für Kaspersky Endpoint Security enthält.

Zu den Update-Quellen gehören der Kaspersky-Security-Center-Server, die Kaspersky-Update-Server sowie Netzwerkordner und lokale Ordner.

Standardmäßig enthält die Liste für Update-Quellen den Server von Kaspersky Security Center und die Kaspersky-Update-Server. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden.

Kaspersky Endpoint Security unterstützt keine Updates von HTTPS-Servern, außer es sind Kaspersky-Update-Server.

Wurden mehrere Ressourcen als Update-Quellen gewählt, greift Kaspersky Endpoint Security bei einer Aktualisierung streng der Reihe nach darauf zu. Bei der Update-Aufgabe wird das Update-Paket aus der ersten verfügbaren Update-Quelle verwendet.

Gehen Sie folgendermaßen vor, um eine Update-Quelle hinzuzufügen:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.
2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.
3. Klicken Sie auf die Schaltfläche **Update-Quellen anpassen**.
4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
5. Geben Sie im folgenden Fenster die Adresse des FTP- oder HTTP-Servers, des Netzwerkordners oder lokalen Ordners an, der das Update-Paket enthält.

   Das Format für den Pfad einer Update-Quelle sieht wie folgt aus:

   - Geben Sie für einen FTP- oder HTTP-Server die Webadresse oder die IP-Adresse der Website ein.

     Beispielsweise `http://dnl-01.geo.kaspersky.com/` oder `93.191.13.103`.

     Für einen FTP-Server ist die Angabe der Anmeldeparameter in folgendem Format möglich: `ftp://<Benutzername>:<Kennwort>@<Knoten>:<Port>`.

   - Geben Sie für einen Netzwerkordner den UNC-Pfad ein.

     Beispiel: `\\Server\Share\Update distribution`.

   - Geben Sie für einen lokalen Ordner den vollständigen Ordnerpfad ein.

     Zum Beispiel, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.
6. Klicken Sie auf **Auswählen**.
7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.
8. Speichern Sie die vorgenommenen Änderungen.

Update aus dem gemeinsamen Ordner anpassen

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update der Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus einem gemeinsamen Ordner erfolgen soll. Dazu lädt ein Computer des lokalen Unternehmensnetzwerks die Update-Pakete vom Administrationsserver für Kaspersky Security Center oder von den Kaspersky-Update-Servern herunter und kopiert das heruntergeladene Update-Paket in einen gemeinsamen Ordner. In diesem Fall können die übrigen Computer des lokalen Unternehmensnetzwerks das Update-Paket aus dem gemeinsamen Ordner abrufen.

Um das Update der Datenbanken und Programm-Module aus einem gemeinsamen Ordner einzurichten, sind folgende Schritte erforderlich:

1. Kopieren des Update-Pakets in einen gemeinsamen Ordner auf einem Computer des lokalen Firmennetzwerks aktivieren

2. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten gemeinsamen Ordner für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks.

Gehen Sie folgendermaßen vor, um den Modus zur Verteilung des Update-Pakets aus einem gemeinsamen Ordner zu aktivieren:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.

2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.

3. Aktivieren Sie im Abschnitt **Verteilen der Updates** das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

4. Geben Sie den UNC-Pfad des gemeinsamen Ordners an (Beispiel: `\\Server\Share\Update distribution`).

5. Speichern Sie die vorgenommenen Änderungen.

Um das Update aus einem gemeinsamen Ordner anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.

2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.

3. Klicken Sie auf die Schaltfläche **Update-Quellen anpassen**.

4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

5. Geben Sie im folgenden Fenster den Pfad des gemeinsamen Ordners an.

   Die Adresse der Quelle muss mit der Adresse übereinstimmen, die zuvor angegeben wurde, als das Kopieren des Update-Pakets in einen gemeinsamen Ordner angepasst wurde (s. *Anleitung oben*).

6. Klicken Sie auf **Auswählen**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

8. Speichern Sie die vorgenommenen Änderungen.

Aktualisierung von Programm-Modulen

Programm-Modul-Updates beheben Fehler, verbessern die Leistung und fügen neue Funktionen hinzu. Wenn ein neues Programm-Modul-Update verfügbar wird, müssen Sie die Installation des Updates bestätigen. Sie können die Installation eines Programm-Modul-Updates entweder in der Programmoberfläche oder im Kaspersky Security Center bestätigen. Wenn ein Update verfügbar wird, zeigt das Programm im Hauptfenster von Kaspersky Endpoint Security eine der folgenden Benachrichtigungen an: wichtiges Update () oder kritisches Update (). Falls für ein Programm-Modul-Update zuerst ein Lizenzvertrag gelesen und bestätigt werden muss, dann installiert das Programm das Update erst nach der Zustimmung zum Lizenzvertrag. Einzelheiten über die Verfolgung von Programm-Modul-Updates und die Bestätigung eines Updates im Kaspersky Security Center *finden Sie in der Hilfe zum Kaspersky Security Center*.

Nach der Installation eines Programm-Updates kann es erforderlich sein, dass Sie Ihren Computer neu starten müssen.

Um das Update für Programm-Module anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.
2. Wählen Sie die Aufgabe *Update* und klicken Sie auf den Link **Ausführungsmodus: <Modus>**.

   Die Eigenschaften der Aufgabe *Update* werden geöffnet.
3. Aktivieren Sie im Block **Updates für Programm-Module herunterladen und installieren** das Kontrollkästchen **Updates für Programm-Module herunterladen**.
4. Wählen Sie die Programm-Modul-Updates aus, die Sie installieren möchten.

   - **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde.
   - **Nur bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.
5. Speichern Sie die vorgenommenen Änderungen.

Verwendung eines Proxyservers beim Update

Für den Download von Updates der Datenbanken und Programm-Module kann die Angabe von Proxyserver-Einstellungen erforderlich sein. Wenn mehrere Update-Quellen vorhanden sind, werden die Proxyserver-Einstellungen für alle Quellen verwendet. Wenn für bestimmte Update-Quellen kein Proxyserver erforderlich ist, können Sie die Verwendung des Proxyservers in den Richtlinieneigenschaften deaktivieren. Kaspersky Endpoint Security verwendet den Proxyserver auch für den Zugriff auf Kaspersky Security Network und auf die Aktivierungsserver.

Um die Verbindung mit den Update-Quellen über einen Proxyserver anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster von „Web Console“ auf ⚙.

   Das Eigenschaftsfenster des Administrationsservers wird geöffnet.

2. Wechseln Sie zum Abschnitt **Einstellungen für den Internetzugriff konfigurieren**.

3. Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden**.

4. Passen Sie die Einstellungen für die Verbindung mit dem Proxyserver an: Adresse des Proxyservers, Port und Authentifizierungseinstellungen (Benutzername und Kennwort).

5. Klicken Sie auf **Speichern**.

Um die Verwendung des Proxyservers für eine bestimmte Administrationsgruppe zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Verwendung des Proxyservers deaktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen → Netzwerkeinstellungen**.

5. Wählen Sie im Block **Proxyserver-Einstellungen** die Variante **Proxyserver nicht verwenden** aus.

6. Klicken Sie auf **OK**.

7. Bestätigen Sie die Änderungen durch Klick auf **Speichern**.

So konfigurieren Sie die Proxyserver-Einstellungen in der Programmoberfläche:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.

3. Klicken Sie im **Proxyserver**-Block auf den Link **Proxyserver-Einstellungen**.

4. Wählen Sie im geöffneten Fenster eine der folgenden Varianten aus, nach welcher die Adresse des Proxyservers ermittelt werden soll:

   - **Proxyserver-Einstellungen automatisch ermitteln**.

     Dieser Status gilt als Standard. Kaspersky Endpoint Security verwendet die Proxyserver-Einstellungen, die in den Betriebssystemeinstellungen definiert sind.

   - **Folgende Proxyserver-Einstellungen verwenden**.

     Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die Einstellungen für die Verbindung mit dem Proxyserver: Proxyserver-Adresse und Port.

5. Wenn Sie die Authentifizierung auf dem Proxyserver aktivieren möchten, aktivieren Sie das Kontrollkästchen **Proxyserver-Authentifizierung verwenden** und geben Sie Ihre Benutzerkonto-Anmeldedaten an.

6. Damit der Proxyserver nicht verwendet wird, wenn die Datenbanken und Programm-Module aus einem gemeinsamen Ordner aktualisiert werden, aktivieren Sie das Kontrollkästchen **Für lokale Adressen keinen**

Proxyserver verwenden.

7. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen wird Kaspersky Endpoint Security den Proxyserver zum Herunterladen von Programmmodul- und Datenbanken-Updates verwenden. Kaspersky Endpoint Security wird den Proxyserver auch für den Zugriff auf KSN-Server und Kaspersky-Aktivierungsserver verwenden. Wenn eine Authentifizierung auf dem Proxyserver erforderlich ist, aber die Anmeldedaten für das Benutzerkonto nicht angegeben wurden oder falsch sind, fordert Kaspersky Endpoint Security Sie auf, den Benutzernamen und das Kennwort einzugeben.

Rollback des letzten Updates

Nach dem ersten Update der Datenbanken und Programm-Module steht eine Rollback-Funktion zur Verfügung, mit der Sie zu den vorherigen Datenbanken und Programm-Modulen zurückkehren können.

Jedes Mal, wenn der Benutzer das Update startet, erstellt Kaspersky Endpoint Security zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt dann mit der Aktualisierung. Somit kann bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückgekehrt werden. Die Rollback-Funktion für das letzte Update ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert.

Gehen Sie folgendermaßen vor, um das letzte Update rückgängig zu machen:

1. Klicken Sie im Programmhauptfenster auf **Datenbanken-Update**.

2. Klicken Sie im Block **Rollback von Datenbanken auf ihre vorherige Version ausführen** auf **Rollback**.

Kaspersky Endpoint Security beginnt mit dem Zurücksetzen des letzten Datenbanken-Updates. Das Programm zeigt den Rollback-Fortschritt, die Größe der heruntergeladenen Dateien und die Update-Quelle an. Sie können jederzeit auf die Schaltfläche  klicken, um diese Aufgabe zu beenden.

Um von der einfachen Programmoberfläche aus eine Aufgabe zum Update-Rollback zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.

2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:

- Wählen Sie eine nicht gestartete Aufgabe zum Update-Rollback aus, um sie zu starten.
- Wählen Sie eine laufende Aufgabe zum Update-Rollback aus, um sie abzubrechen.
- Wählen Sie eine angehaltene Aufgabe zum Update-Rollback aus, um sie erneut zu starten.

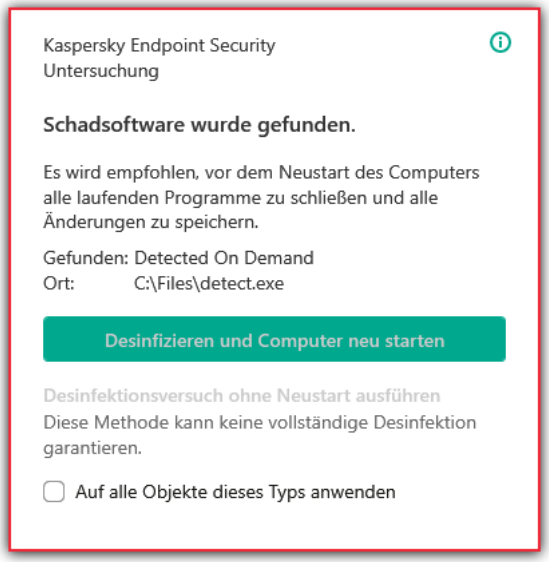
Arbeit mit aktiven Bedrohungen

Kaspersky Endpoint Security protokolliert Informationen über Dateien, die aus bestimmten Gründen nicht verarbeitet wurden. Diese Informationen werden als Ereignisse in die Liste der aktiven Bedrohungen eingetragen. Zur Verarbeitung aktiver Bedrohungen verwendet Kaspersky Endpoint Security die Technologie zur aktiven Desinfektion. Die „Aktive Desinfektion" funktioniert auf Workstations und Servern in unterschiedlicher Weise. Die Technologie zur aktiven Desinfektion können Sie in den Einstellungen der Aufgabe *Untersuchung auf Viren* und in den Programmeinstellungen anpassen.

Desinfektion aktiver Bedrohungen auf Workstations

Um aktive Bedrohungen auf Workstations verarbeiten zu können, aktivieren Sie die Technologie zur aktiven Desinfektion in den Programmeinstellungen. Konfigurieren Sie als Nächstes die Benutzererfahrung in den Eigenschaften der Aufgabe *Untersuchung auf Viren*. In den Aufgabeneigenschaften finden Sie ein Kontrollkästchen mit dem Titel **Sofortige aktive Desinfektion aktivieren**. Ist das Kontrollkästchen aktiviert, so führt Kaspersky Endpoint Security eine Desinfektion aus, ohne den Benutzer zu benachrichtigen. Nach Abschluss der Desinfektion wird der Computer neu gestartet. Ist das Kontrollkästchen deaktiviert, zeigt Kaspersky Endpoint Security eine Benachrichtigung über eine aktive Bedrohung an (s. Abb. unten). Sie können diese Benachrichtigung nicht schließen, ohne die Datei zu verarbeiten.

Wenn auf dem Computer eine Untersuchungsaufgabe ausgeführt wird, erfolgt nur dann eine aktive Desinfektion, wenn in den Eigenschaften der Richtlinie, die für diesen Computer gilt, die Aktive Desinfektion aktiviert ist.



Benachrichtigung über eine aktive Bedrohung

Desinfektion aktiver Bedrohungen auf Servern

Gehen Sie wie folgt vor, um aktive Bedrohungen auf Servern zu verarbeiten:

- Aktivieren Sie die Technologie zur aktiven Desinfektion in den Programmeinstellungen.
- Aktivieren Sie die sofortige aktive Desinfektion in den Eigenschaften der Aufgabe *Untersuchung auf Viren*.

Wenn Kaspersky Endpoint Security auf einem Computer mit Windows für Server installiert ist, zeigt Kaspersky Endpoint Security keine Benachrichtigung an. Deshalb kann der Benutzer keine Aktion zur Desinfektion einer aktiven Bedrohung auswählen. Um eine Bedrohung zu desinfizieren, aktivieren Sie die Technologie zur aktiven Desinfektion in den Programmeinstellungen und aktivieren Sie die sofortige aktive Desinfektion in den Einstellungen der Aufgabe *Untersuchung auf Viren*. Anschließend müssen Sie die Aufgabe *Untersuchung auf Viren* starten.

Verarbeitung aktiver Bedrohungen

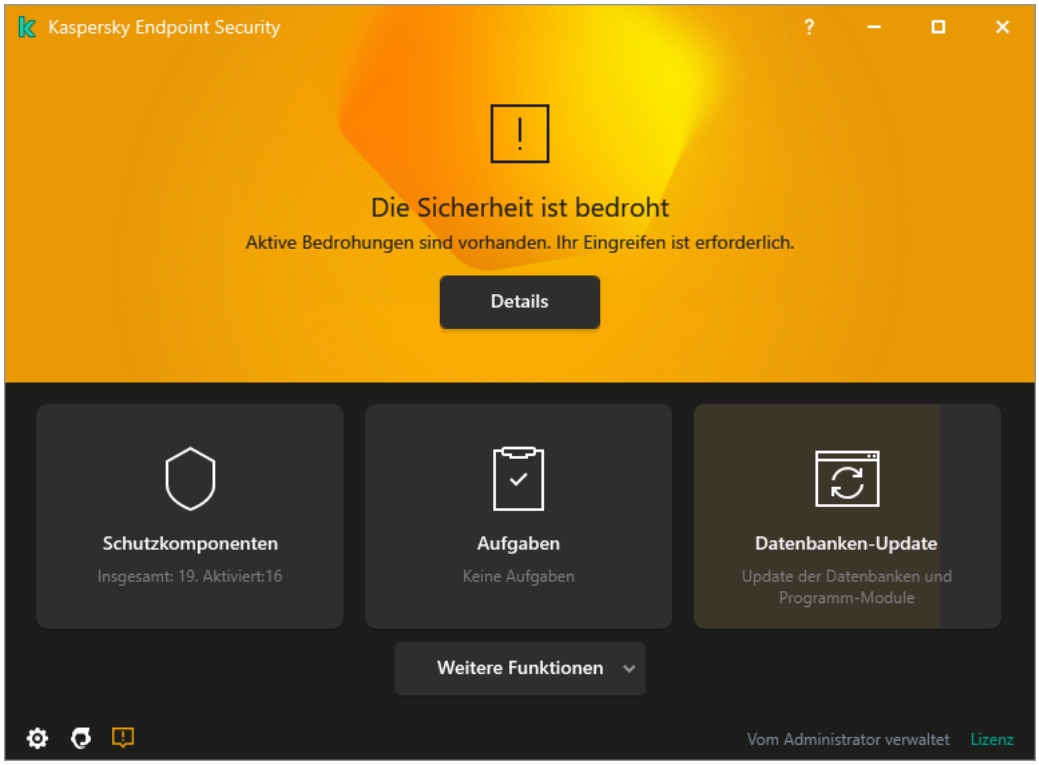
Eine infizierte Datei gilt dann als *verarbeitet*, wenn Kaspersky Endpoint Security diese Datei im Zuge der Untersuchung des Computers auf Viren und andere Schadprogramme gemäß den Programmeinstellungen einer der folgenden Aktionen unterzogen hat:

- Desinfizieren.
- Löschen
- Löschen, wenn Desinfektion fehlschlägt.

Kaspersky Endpoint Security setzt die Datei auf die Liste der aktiven Bedrohungen, falls Kaspersky Endpoint Security bei der Untersuchung des Computers auf Viren und andere bedrohliche Programme mit dieser Datei eine Aktion ausgeführt hat, welche nicht in den Programmeinstellungen vorgesehen ist.

Dies ist in folgenden Fällen möglich:

- Die zu untersuchende Datei ist nicht verfügbar (Sie befindet sich beispielsweise auf einem Netzlaufwerk oder einem externen Laufwerk ohne Schreibrechte).
- In den Programmeinstellungen ist für Untersuchungsaufgaben im Abschnitt **Aktion beim Fund einer Bedrohung** die Aktion **Informieren** ausgewählt, und der Benutzer hat nach Anzeige der Meldung über eine infizierte Datei die Option **Überspringen** ausgewählt.



Programmhauptfenster, wenn eine Bedrohung erkannt wurde

Um aktive Bedrohungen zu verarbeiten:

1. Klicken Sie im Programmhauptfenster auf **Details**.

   Die Liste der aktive Bedrohungen wird geöffnet.

2. Wählen Sie das Objekt aus, das Sie verarbeiten möchten.

3. Legen Sie fest, wie die Bedrohung behandelt werden soll:

   - **Beheben**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht.

   - **Ignorieren**. Wenn diese Option ausgewählt wird, löscht Kaspersky Endpoint Security den Eintrag aus der Liste der aktive Bedrohungen. Wenn die Liste keine aktiven Bedrohungen mehr enthält, ändert sich der Computerstatus in *OK*. Wenn das Objekt erneut gefunden wird, fügt Kaspersky Endpoint Security einen neuen Eintrag zur Liste der aktiven Bedrohungen hinzu.

   - **Enthaltenden Ordner öffnen**. Wenn diese Option ausgewählt wird, öffnet Kaspersky Endpoint Security im Dateimanager den Ordner, der das Objekt enthält. Dann können Sie das Objekt entweder manuell löschen oder das Objekt in einen Ordner außerhalb des Schutzbereichs verschieben.

   - **Details**. Wenn diese Option ausgewählt wird, öffnet Kaspersky Endpoint Security die Website der Kaspersky-Viren-Enzyklopädie.

Schutz vor bedrohlichen Dateien

Die Komponente „Schutz vor bedrohlichen Dateien“ schützt das Dateisystem des Computers vor einer Infektion. Die Komponente „Schutz vor bedrohlichen Dateien“ befindet sich standardmäßig permanent im Arbeitsspeicher des Computers. Die Komponente untersucht die Dateien auf allen Laufwerken des Computers sowie auf verbundenen Datenträgern. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Die Komponente untersucht die Dateien, auf die der Benutzer oder ein Programm zugreift. Beim Fund einer schädlichen Datei blockiert Kaspersky Endpoint Security den Vorgang mit dieser Datei. Das Programm desinfiziert oder löscht die schädliche Datei. Das Vorgehen ist von den Einstellungen der Komponente „Schutz vor bedrohlichen Dateien“ abhängig.

Beim Zugriff auf eine Datei, deren Inhalt sich im Cloud-Speicher OneDrive befindet, lädt Kaspersky Endpoint Security den Inhalt dieser Datei herunter und untersucht ihn.

Schutz vor bedrohlichen Dateien aktivieren und deaktivieren

Die Komponente „Schutz vor bedrohlichen Dateien“ ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Zum Schutz vor bedrohlichen Dateien kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungssätze, die im Programm gespeichert sind, heißen *Sicherheitsstufen*: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Um die Komponente „Schutz vor bedrohlichen Dateien“ zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.
3. Verwenden Sie den Schalter **Schutz vor bedrohlichen Dateien**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Wenn Sie die Komponente aktiviert haben, führen Sie im Abschnitt **Sicherheitsstufe** einen der folgenden Schritte aus:
   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:
     - **Hoch**. Auf dieser Sicherheitsstufe für Dateien kontrolliert die Komponente „Schutz vor bedrohlichen Dateien“ alle Dateien, die geöffnet, gespeichert und gestartet werden, mit höchster Genauigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht alle Dateitypen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Untersucht werden außerdem Archive, Installationspakete und eingebettete OLE-Objekte.

- **Empfohlen**. Diese Sicherheitsstufe für Dateien wird von Kaspersky-Experten empfohlen. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht Archive oder Installationspakete nicht. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.

- **Niedrig**. Diese Sicherheitsstufe für Dateien bietet eine maximale Untersuchungsgeschwindigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden von der Komponente „Schutz vor bedrohlichen Dateien“ nicht untersucht.

- Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Einstellungen für die Komponenten fest.

  Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen, indem Sie auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen** im oberen Teil des Fensters klicken.

5. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor bedrohlichen Dateien (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Dateitypen	**Dateien nach Format untersuchen**	Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht.
Heuristische Analyse	**Oberflächlich**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Nur neue und veränderte Dateien untersuchen	**Aktiviert**	Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.
iSwift-Technologie	**Aktiviert**	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie

		iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie	**Aktiviert**	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Dateien in Microsoft Office-Formaten untersuchen	**Aktiviert**	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Untersuchungsmodus	**Intelligent**	In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien“-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.
Aktion beim Fund einer Bedrohung	**Desinfizieren, irreparable Objekte löschen**	Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht.

Schutz vor bedrohlichen Dateien automatisch anhalten

Sie können festlegen, dass der Schutz vor bedrohlichen Dateien zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Es gilt als Notlösung, den Schutz vor bedrohlichen Dateien bei einem Konflikt mit bestimmten Programmen anzuhalten. Sollten während des Betriebs einer Komponente Konflikte auftreten, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky zu wenden. Die Experten helfen Ihnen dabei, eine Lösung für die gleichzeitige Verwendung der Komponente „Schutz vor bedrohlichen Dateien“ mit anderen Programmen auf Ihrem Computer zu finden.

Um das automatische Anhalten des Schutzes vor bedrohlichen Dateien anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Klicken Sie im Block **Schutz vor bedrohlichen Dateien anhalten** auf den Link **Schutz vor bedrohlichen Dateien anhalten**.

5. Konfigurieren Sie im geöffneten Fenster die Einstellungen für das Anhalten des Schutzes vor bedrohlichen Dateien:

   a. Konfigurieren Sie einen Zeitplan für das automatische Anhalten des Schutzes vor bedrohlichen Dateien.

   b. Erstellen Sie eine Liste von Programmen, deren Ausführung bewirken soll, dass der Schutz vor bedrohlichen Dateien seine Aktivitäten unterbricht.

6. Speichern Sie die vorgenommenen Änderungen.

Ändern der Aktion, welche die Komponente „Schutz vor bedrohlichen Dateien“ mit infizierten Dateien ausführen soll

Die Komponente „Schutz vor bedrohlichen Dateien“ versucht standardmäßig, alle gefundenen infizierten Dateien automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden diese Dateien von der Komponente „Schutz vor bedrohlichen Dateien“ gelöscht.

Zum Ändern der Aktion, welche die Komponente „Schutz vor bedrohlichen Dateien“ mit infizierten Dateien ausführen soll, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die entsprechende Option:

   - **Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht.

   - **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.

   - **Blockieren** Wenn diese Variante ausgewählt ist, blockiert die Komponente „Schutz vor bedrohlichen Dateien“ die infizierten Dateien automatisch, ohne einen Desinfektionsversuch zu unternehmen.

   Bevor Sie versuchen, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt Kaspersky Endpoint Security eine Sicherungskopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

4. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich für die Komponente „Schutz vor bedrohlichen Dateien"

Der Begriff Schutzbereich bezieht sich auf die Objekte, die von einer Komponente während ihrer Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente „Schutz vor bedrohlichen Dateien" wird durch die Eigenschaften Speicherort und Typ der zu untersuchenden Dateien definiert. Die Komponente „Schutz vor bedrohlichen Dateien" untersucht standardmäßig nur infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers aus gestartet werden.

Bei der Auswahl des Typs für die zu untersuchenden Dateien sollte Folgendes beachtet werden:

1. Für bestimmte Dateiformate (z. B. TXT-Format) besteht eine geringe Wahrscheinlichkeit, dass schädlicher Code eindringt und dann aktiviert wird. Es gibt aber auch Dateiformate, die ausführbaren Code enthalten (z. B. die Formate EXE und DLL). Ausführbarer Code kann auch in Dateiformaten enthalten sein, die dafür nicht vorgesehen sind (z. B. das Format DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist hoch.

2. Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in TXT geändert wurde, an Ihren Computer senden. Wenn Sie die Dateiuntersuchung nach Erweiterung festgelegt haben, überspringt das Programm eine solche Datei bei der Untersuchung. Wenn die Überprüfung von Dateien nach Format ausgewählt wird, analysiert Kaspersky Endpoint Security den Datei-Header unabhängig von seiner Erweiterung. Falls sich ergibt, dass die Datei das Format einer ausführbaren Datei (beispielsweise EXE) besitzt, so wird die Datei untersucht.

Gehen Sie folgendermaßen vor, um einen Schutzbereich zu erstellen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Geben Sie im Block **Dateitypen** den Typ der Dateien an, die von der Komponente „Schutz vor bedrohlichen Dateien" untersucht werden sollen:

   - **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung).

   - **Dateien nach Format untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht.

   - **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.

5. Klicken Sie auf den Link **Schutzbereich ändern**.

6. Wählen Sie im geöffneten Fenster die Objekte aus, die Sie dem Schutzbereich hinzufügen oder von diesem ausschließen möchten.

   Objekte, die standardmäßig zum Schutzbereich gehören, können weder gelöscht noch geändert werden.

7. Um ein neues Objekt zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

      Der Ordnerbaum wird geöffnet.

   b. Wählen Sie ein Objekt und klicken Sie auf **Auswählen**.

   Sie können ein Objekt von Untersuchungen ausschließen, ohne es aus der Liste der Objekte im Untersuchungsbereich zu löschen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

8. Speichern Sie die vorgenommenen Änderungen.

Untersuchungsmethoden verwenden

Kaspersky Endpoint Security verwendet die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse. Bei der Signaturanalyse vergleicht Kaspersky Endpoint Security ein gefundenes Objekt mit den Einträgen in den Programm-Datenbanken. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.

Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.

Um die Verwendung der heuristischen Analyse für die Komponente „Schutz vor bedrohlichen Dateien“ anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wenn Sie möchten, dass das Programm die heuristische Analyse zum Schutz vor Dateibedrohungen verwendet, aktivieren Sie das Kontrollkästchen **Heuristische Analyse** im Block **Untersuchungsmethoden**. Legen Sie dann mit dem Schieberegler die Stufe der heuristischen Analyse fest: **oberflächlich**, **mittel** oder **tief**.

5. Speichern Sie die vorgenommenen Änderungen.

Verwendung von Untersuchungstechnologien durch die Komponente „Schutz vor bedrohlichen Dateien”

Um die Verwendung der Untersuchungstechnologien für die Komponente „Schutz vor bedrohlichen Dateien“ anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

   - **iSwift-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - **iChecker-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

5. Speichern Sie die vorgenommenen Änderungen.

Dateiuntersuchung optimieren

Um die Dateiuntersuchung mit der Komponente „Schutz vor bedrohlichen Dateien“ zu optimieren, können Sie die Untersuchungsdauer verkürzen und die Leistung von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Sie können außerdem die Technologien iChecker und iSwift aktivieren, mit denen sich die Dateiuntersuchung beschleunigen lässt. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit der letzten Untersuchung nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Untersuchung von Dateien zu optimieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie unter **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

5. Speichern Sie die vorgenommenen Änderungen.

Untersuchung von zusammengesetzten Dateien

Eine häufig anzutreffende Methode zum Verstecken von Viren und anderen gefährlichen Programmen ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive oder Datenbanken. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

Die Verarbeitungsmethode für eine zusammengesetzte infizierte Datei (Löschen oder Desinfektion) ist vom Dateityp abhängig.

Die Komponente „Schutz vor bedrohlichen Dateien“ desinfiziert zusammengesetzte Dateien der Formate RAR, ARJ, ZIP, CAB und LHA, und löscht Dateien aller übrigen Formate (unter Ausnahme von E-Mail-Datenbanken).

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Installationspakete oder Office-Format-Dateien.
5. Wenn die Untersuchung nur neuer und geänderter Dateien deaktiviert ist, konfigurieren Sie die Einstellungen für die Untersuchung jedes Typs von zusammengesetzten Dateien: „Alle Dateien dieses Typs untersuchen“ oder „Nur neue Dateien untersuchen“.

   Wenn die Untersuchung nur neuer und geänderter Dateien aktiviert ist, überprüft Kaspersky Endpoint Security nur neue und geänderte Dateien aller Arten von zusammengesetzten Dateien.
6. Konfigurieren Sie die erweiterten Einstellungen für die Untersuchung von zusammengesetzten Dateien.

   - **Große zusammengesetzte Dateien nicht entpacken**.

     Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe.

     Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

   - **Zusammengesetzte Dateien im Hintergrund entpacken**.

Wenn das Kontrollkästchen aktiviert ist, gewährt Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, die größer sind als der festgelegte Wert. Der Zugriff wird gewährt, bevor diese Dateien untersucht werden. Dabei entpackt und untersucht Kaspersky Endpoint Security die zusammengesetzten Dateien im Hintergrundmodus.

Kaspersky Endpoint Security gewährt den Zugriff auf zusammengesetzte Dateien, die kleiner sind als der festgelegte Wert. Der Zugriff wird erst gewährt, nachdem diese Dateien entpackt und untersucht wurden.

Wenn das Kontrollkästchen deaktiviert ist, gewährt Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, erst nachdem die Dateien beliebiger Größe entpackt und untersucht wurden.

7. Speichern Sie die vorgenommenen Änderungen.

Untersuchungsmodus für Dateien ändern

Untersuchungsmodus bedeutet eine Bedingung, unter welcher die Komponente „Schutz vor bedrohlichen Dateien“ die Untersuchung einer Datei starten soll. Kaspersky Endpoint Security verwendet standardmäßig den intelligenten Untersuchungsmodus für Dateien. Um zu entscheiden, ob eine Untersuchung von Dateien erforderlich ist, analysiert die Komponente „Schutz vor bedrohlichen Dateien“ in diesem Modus die Vorgänge, die von einem Benutzer, von einem Programm im Auftrag eines Benutzers (mit dessen Benutzerdaten eine Anmeldung im Betriebssystem erfolgte, oder eines anderen Benutzers) oder vom Betriebssystem ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Word-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Dateien zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wählen Sie unter **Untersuchungsmodus** den erforderlichen Modus:

   - **Intelligent**. In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien“-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

   - **Bei Zugriff und Veränderungen**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ Objekte jedes Mal untersucht, wenn versucht wird, diese zu öffnen oder zu bearbeiten.

   - **Bei Zugriff**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu öffnen.

   - **Bei Ausführung**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu starten.

5. Speichern Sie die vorgenommenen Änderungen.

Schutz vor Web-Bedrohungen

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert schädliche Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Kaspersky Endpoint Security untersucht den HTTP-, HTTPS- und FTP-Datenverkehr. Kaspersky Endpoint Security untersucht URL- und IP-Adressen. Sie können die Ports angeben, die Kaspersky Endpoint Security kontrollieren soll, oder alle Ports auswählen.

Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

Wenn ein Benutzer versucht, eine schädliche Website oder eine Phishing-Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).

Benachrichtigung über ein Verbot des Zugriffs auf die Website

Schutz vor Web-Bedrohungen aktivieren und deaktivieren

Die Komponente „Schutz vor Web-Bedrohungen“ ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Zum Schutz vor Web-Bedrohungen kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungssätze, die im Programm gespeichert sind, heißen *Sicherheitsstufen*: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** für den Web-Datenverkehr gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen für den Web-Datenverkehr wählen, der mit den Protokollen HTTP und FTP empfangen oder übertragen wird, oder die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr selbstständig anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Um die Komponente „Schutz vor Web-Bedrohungen“ zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz** → **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
3. Verwenden Sie den Schalter **Schutz vor Web-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Wenn Sie die Komponente aktiviert haben, führen Sie im Abschnitt **Sicherheitsstufe** einen der folgenden Schritte aus:
   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:
     - **Hoch**. Auf dieser Sicherheitsstufe für den Web-Datenverkehr untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Web-Datenverkehr, der über die Protokolle HTTP und FTP empfangen wird, mit höchster Genauigkeit. Der Schutz vor Web-Bedrohungen untersucht alle Objekte des Web-Datenverkehrs ausführlich, verwendet die vollständigen Programm-Datenbanken und führt zusätzlich eine heuristische Analyse mit maximaler Tiefe aus.
     - **Empfohlen**. Diese Sicherheitsstufe für den Web-Datenverkehr bietet ein optimales Verhältnis zwischen der Leistung von Kaspersky Endpoint Security und der Sicherheit für den Web-Datenverkehr. Die Komponente „Schutz vor Web-Bedrohungen“ führt die heuristische Analyse auf der Stufe **Mittel** aus. Diese Sicherheitsstufe für den Web-Datenverkehr wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.
     - **Niedrig**. Diese Sicherheitsstufe für den Web-Datenverkehr gewährleistet maximale Geschwindigkeit bei der Untersuchung des Web-Datenverkehrs. Die Komponente „Schutz vor Web-Bedrohungen“ führt die heuristische Analyse auf der Stufe **Oberflächlich** aus.
   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Einstellungen für die Komponenten fest.

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen, indem Sie auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen** im oberen Teil des Fensters klicken.
5. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor Web-Bedrohungen (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Links mit der Datenbank für bösartige Webadressen untersuchen	**Aktiviert**	Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Webadresse mit der Datenbank für Phishing-Webadressen untersuchen	**Aktiviert**	Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Heuristische	**Mittlere**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der

Analyse verwenden (Schutz vor Web-Bedrohungen)	**Untersuchung**	aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Heuristische Analyse verwenden (Anti-Phishing)	**Aktiviert**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.
Aktion beim Fund einer Bedrohung	**Download verbieten**	Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

Aktion für schädliche Objekte im Web-Datenverkehr ändern

Wenn ein infiziertes Objekt im Web-Datenverkehr gefunden wird, blockiert die Komponente „Schutz vor Web-Bedrohungen“ standardmäßig den Zugriff auf das Objekt und zeigt eine Bildschirmmeldung über die Sperrung an.

Gehen Sie folgendermaßen vor, um die Aktion für schädliche Objekte im Web-Datenverkehr zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor Web-Bedrohungen** aus.
3. Wählen Sie unter **Aktion beim Fund einer Bedrohung** eine Aktion, die Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr ein schädliches Objekt gefunden wird:
   - **Download verbieten**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.
   - **Informieren** Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.
4. Speichern Sie die vorgenommenen Änderungen.

URLs gegen Datenbanken mit Phishing- und bösartigen Web-Adressen untersuchen

Durch eine Untersuchung von Links auf Phishing-Webadressen lassen sich *Phishing-Angriffe* vermeiden. Ein häufiges Beispiel für Phishing-Angriffe ist eine E-Mail-Nachricht, die scheinbar von Ihrer Bank stammt und einen Link zur offiziellen Website der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Website, die eine exakte Kopie der Bankseite darstellt und für die im Browser sogar deren Webadresse angezeigt wird, obwohl Sie sich in Wirklichkeit auf einer fiktiven Website befinden. Alle Aktionen, die Sie auf dieser Website ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Da sich ein Phishing-Link nicht nur in E-Mail-Nachrichten, sondern beispielsweise auch im Text einer ICQ-Nachricht befinden kann, überwacht die Komponente „Schutz vor Web-Bedrohungen" alle Versuche zum Öffnen einer Phishing-Website auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Websites. Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky Endpoint Security.

Um in der Komponente „Schutz vor Web-Bedrohungen" die Link-Untersuchung anzupassen, bei der die Datenbanken für Phishing-Webadressen und schädliche Adressen verwendet werden:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz** → **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Gehen Sie wie folgt vor:

   - Damit die Komponente „Schutz vor Web-Bedrohungen" Links mithilfe der Datenbanken für bösartige Webadressen untersucht, aktivieren Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **URL mit der Datenbank für bösartige URLs untersuchen**. Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.

     Kaspersky Endpoint untersucht alle Links, um festzustellen, ob sie in Datenbanken mit bösartigen Webadressen aufgeführt sind. Die Programmeinstellungen für die Untersuchung sicherer Verbindungen haben keinen Einfluss auf die Link-Untersuchungsfunktion. Mit anderen Worten: Wenn Untersuchungen verschlüsselter Verbindungen deaktiviert sind, prüft Kaspersky Endpoint Security Links anhand von Datenbanken mit bösartigen Web-Adressen, selbst wenn der Netzwerkverkehr über eine verschlüsselte Verbindung übertragen wird.

   - Damit die Komponente „Schutz vor Web-Bedrohungen" Links mithilfe der Datenbanken für Phishing-Webadressen untersucht, aktivieren Sie im Block **Anti-Phishing** das Kontrollkästchen **URL mit der Datenbank für Phishing-URLs untersuchen**. Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.

Zur Untersuchung von Links können Sie auch die Reputations-Datenbanken von Kaspersky Security Network verwenden.

5. Speichern Sie die vorgenommenen Änderungen.

Verwendung der heuristischen Analyse durch die Komponente „Schutz vor Web-Bedrohungen"

Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann Bedrohungen erkennen, über die noch keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse anzupassen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz** → **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Aktivieren Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse verwenden**, wenn das Programm beim Untersuchen des Web-Verkehrs auf Viren und andere Malware eine heuristische Analyse verwenden soll. Legen Sie dann mit dem Schieberegler die Stufe der heuristischen Analyse fest: **oberflächlich**, **mittel** oder **tief**.
5. Aktivieren Sie im Block **Anti-Phishing** das Kontrollkästchen **Heuristische Analyse verwenden**, wenn Sie möchten, dass das Programm beim Untersuchen von Webseiten nach Phishing-Links eine heuristische Analyse verwendet.
6. Speichern Sie die vorgenommenen Änderungen.

Liste mit vertrauenswürdigen Webadressen erstellen

Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vertrauen. Informationen, die von vertrauenswürdigen Webadressen stammen, werden von der Komponente „Schutz vor Web-Bedrohungen" nicht auf Viren und andere gefährliche Programme analysiert. Diese Option kann beispielsweise nützlich sein, wenn die Komponente „Schutz vor Web-Bedrohungen" den Download einer Datei von einer Ihnen bekannten Website verhindert.

Der Begriff Webadresse bezieht sich sowohl auf eine bestimmte Webseite, als auch auf eine Website.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Webadressen anzulegen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor Web-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen**.

   Ist das Kontrollkästchen aktiviert, so untersucht die Komponente „Schutz vor Web-Bedrohungen" den Inhalt von Webseiten/Websites nicht, deren Adressen auf der Liste der vertrauenswürdigen Webadressen stehen. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website.

5. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen.

6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und importieren der Liste vertrauenswürdiger Webadressen

Sie können die Liste der vertrauenswürdigen Webadressen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Sie können die Export-/Import-Funktion auch verwenden, um die Liste der vertrauenswürdigen Webadressen zu sichern oder die Liste auf einen anderen Server zu migrieren.

So exportieren und importieren Sie eine Liste vertrauenswürdiger Webadressen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Web-Bedrohungen** aus.
6. Klicken Sie auf **Einstellungen**.
7. Wählen Sie im geöffneten Fenster die Registerkarte **Vertrauenswürdige Webadressen**.
8. So exportieren Sie eine Liste mit vertrauenswürdigen Webadressen:
   a. Wählen Sie die vertrauenswürdigen Webadressen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine vertrauenswürdige Webadresse ausgewählt haben, exportiert Kaspersky Endpoint Security alle Webadressen.

   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der vertrauenswürdigen Adressen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Webadressen in die XLM-Datei.
9. So importieren Sie die Liste der vertrauenswürdigen Adressen:
   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
10. Speichern Sie die vorgenommenen Änderungen.

[So exportieren und importieren Sie eine Liste vertrauenswürdiger Webadressen in die Web Console und die Cloud-Konsole]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste mit vertrauenswürdigen Webadressen exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
5. So exportieren Sie die Liste der Ausnahmen im Block **Vertrauenswürdige Webadressen**:

   a. Wählen Sie die vertrauenswürdigen Webadressen aus, die Sie exportieren möchten.

   b. Klicken Sie auf **Export**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der vertrauenswürdigen Adressen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Webadressen in die XLM-Datei.
6. So importieren Sie eine Liste von Ausnahmen im Block **Vertrauenswürdige Webadressen**:

   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

Schutz vor E-Mail-Bedrohungen

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente "Schutz vor E-Mail-Bedrohungen" untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. Außerdem überprüft die Komponente, ob Nachrichten bösartige Links oder Phishing-Links enthalten. Die Komponente "Schutz vor E-Mail-Bedrohungen" befindet sich standardmäßig permanent im Arbeitsspeicher des Computers und untersucht alle Nachrichten, die mit den Protokollen POP3, SMTP, IMAP und NNTP oder im Mail-Client Microsoft Office Outlook (MAPI) empfangen oder gesendet werden. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Wenn ein Mail-Client in einem Browser geöffnet ist, untersucht die Komponente "Schutz vor E-Mail-Bedrohungen" die Nachrichten nicht.

Wenn in einer Anlage eine infizierte Datei gefunden wird, ändert Kaspersky Endpoint Security den Nachrichtenbetreff wie folgt: `[Nachricht ist infiziert] <Betreff der Nachricht>` oder `[Infiziertes Objekt wurde gelöscht] <Betreff der Nachricht>`.

Diese Komponente interagiert mit den Mail-Clients, die auf dem Computer installiert sind. Für den Mail-Client Microsoft Office Outlook gibt es eine Erweiterung mit zusätzlichen Einstellungen. Die Erweiterung für die Komponente "Schutz vor E-Mail-Bedrohungen" wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

Schutz vor E-Mail-Bedrohungen aktivieren und deaktivieren

Die Komponente "Schutz vor E-Mail-Bedrohungen" ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Zum Schutz vor E-Mail-Bedrohungen kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungssätze, die im Programm gespeichert sind, heißen *Sicherheitsstufen*: **Hoch**, **Empfohlen**, **Niedrig**. Die E-Mail-Sicherheitsstufe **Empfohlen** gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen für den E-Mail-Schutz wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe für den E-Mail-Schutz geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Um die Komponente "Schutz vor E-Mail-Bedrohungen" zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.
3. Verwenden Sie den Schalter **Schutz vor E-Mail-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Wenn Sie die Komponente aktiviert haben, führen Sie im Abschnitt **Sicherheitsstufe** einen der folgenden Schritte aus:
   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:
     - **Hoch**. Auf dieser E-Mail-Sicherheitsstufe kontrolliert die Komponente „Schutz vor E-Mail-Bedrohungen" die Nachrichten mit höchster Genauigkeit. Die Komponente „Schutz vor E-Mail-Bedrohungen" untersucht ein- und ausgehende E-Mails und führt eine tiefe heuristische Analyse durch. Die E-Mail-Sicherheitsstufe **Hoch** wird für Umgebungen mit hohem Risiko empfohlen. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk ohne zentralisierten E-Mail-Schutz erfolgt.

- **Empfohlen**. Diese E-Mail-Sicherheitsstufe bietet ein optimales Verhältnis zwischen der Leistung von Kaspersky Endpoint Security und der Sicherheit für E-Mails. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mail-Nachrichten und führt eine heuristische Analyse mit mittlerer Tiefe aus. Diese E-Mail-Sicherheitsstufe wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.

- **Niedrig**. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ nur eingehende E-Mail-Nachrichten, führt eine oberflächliche heuristische Analyse aus und scannt die an Nachrichten angehängten Archive nicht. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ E-Mail-Nachrichten mit maximaler Geschwindigkeit und beansprucht die Betriebssystemressourcen minimal. Die E-Mail-Sicherheitsstufe **Niedrig** wird für die Arbeit in einer gut geschützten Umgebung empfohlen. Ein Beispiel für eine solche Umgebung ist ein LAN eines Unternehmens mit zentralisiertem E-Mail-Schutz.

- Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Einstellungen für die Komponenten fest.

  Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen, indem Sie auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen** im oberen Teil des Fensters klicken.

5. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor E-Mail-Bedrohungen (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Schutzbereich	**Eingehende und ausgehende Nachrichten**	Der *Schutzbereich* umfasst Objekte, welche während der Ausführung der Komponente untersucht werden: **Eingehende und ausgehende Nachrichten** oder **Nur eingehende Nachrichten**. Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.
Erweiterung für Microsoft Outlook verbinden	**Aktiviert**	Wenn das Kontrollkästchen aktiviert ist, ist die Untersuchung von E-Mail-Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, aktiviert. Die Untersuchung erfolgt durch die in Microsoft Outlook integrierte Erweiterung. Erfolgt die E-Mail-Untersuchung mithilfe der Erweiterung für Microsoft Outlook, so wird empfohlen, den Exchange-Cache-Modus zu verwenden (Use Cached Exchange Mode). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.
Angehängte Archive untersuchen	**Aktiviert**	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.
Angehängte Office-Format-Dateien untersuchen	**Aktiviert**	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Anlagenfilterung	**Anlagen der ausgewählten Typen umbenennen**	Wenn Sie diese Option auswählen, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Erweiterung angehängter Dateien bestimmter Typen mit einem Unterstrich (z. B. attachment.doc_). Der Benutzer muss die Datei dann zunächst umbenennen, um sie öffnen zu können.

Heuristische Analyse	**Mittlere Untersuchung**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Aktion beim Fund einer Bedrohung	**Desinfizieren, irreparable Objekte löschen**	Wird in einer eingehenden oder ausgehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Konnte das Objekt nicht desinfiziert werden, so löscht Kaspersky Endpoint Security das infizierte Objekt. Kaspersky Endpoint Security fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu: `[Ein infiziertes Objekt wurde gelöscht.] <Nachrichtenbetreff>`.

Aktion für infizierte E-Mail-Nachrichten ändern

Die Komponente "Schutz vor E-Mail-Bedrohungen" versucht standardmäßig, alle gefundenen infizierten E-Mail-Nachrichten automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen" gelöscht.

Um die Aktion für infizierte E-Mail-Nachrichten zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.
3. Wählen Sie im Abschnitt **Aktion beim Fund einer Bedrohung** eine Aktion, die Kaspersky Endpoint Security beim Fund einer infizierten Nachricht ausführen soll:
   - **Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden oder ausgehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Konnte das Objekt nicht desinfiziert werden, so löscht Kaspersky Endpoint Security das infizierte Objekt. Kaspersky Endpoint Security fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu: `[Ein infiziertes Objekt wurde gelöscht.] <Nachrichtenbetreff>`.
   - **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, versieht Kaspersky Endpoint Security den Nachrichtenbetreff mit einer Warnung: `[Message infected] <Nachrichtenbetreff>`. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, so

versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Konnte das Objekt nicht desinfiziert werden, so blockiert Kaspersky Endpoint Security das Senden der Nachricht. Der Mail-Client zeigt einen Fehler an.

- **Blockieren** Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, so fügt Kaspersky Endpoint Security eine Warnung zum Nachrichtenbetreff hinzu: `[Die Nachricht ist infiziert.] <Nachrichtenbetreff>`. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, so blockiert Kaspersky Endpoint Security das Senden der Nachricht. Der Mail-Client zeigt einen Fehler an.

4. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich für die Komponente “Schutz vor E-Mail-Bedrohungen”

Schutzbereich bezieht sich auf die Objekte, die von einer Komponente während der Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“ wird durch folgende Eigenschaften definiert: Einstellungen für die Integration der Komponente „Schutz vor E-Mail-Bedrohungen“ in die Mail-Clients, Typ der E-Mail-Nachrichten und der E-Mail-Protokolle, deren Datenverkehr von der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht wird. Kaspersky Endpoint Security untersucht standardmäßig ein- und ausgehende E-Mail-Nachrichten sowie den Datenverkehr der Mailprotokolle POP3, SMTP, NNTP und IMAP und wird in den Mail-Client Microsoft Office Outlook integriert.

Um den Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“ zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz** → **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wählen Sie im Block **Schutzbereich** die zu untersuchenden Nachrichten aus:

   - **Eingehende und ausgehende Nachrichten**.

   - **Nur eingehende Nachrichten**.

   Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.

   Wenn Sie nur die Untersuchung eingehender Nachrichten wählen, wird empfohlen, eine einmalige Untersuchung aller ausgehenden Nachrichten vorzunehmen, da sich auf Ihrem Computer Mail-Würmer befinden können, die sich mithilfe von E-Mails ausbreiten. Dadurch lassen sich Probleme vermeiden, die durch unkontrolliertes Versenden infizierter Nachrichten von Ihrem Computer auftreten können.

5. Führen Sie im Abschnitt **Integration ins System** folgende Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP untersuchen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten untersucht, die mit den Protokollen POP3,

SMTP, NNTP und IMAP übertragen werden. Die Untersuchung erfolgt, bevor die Nachrichten auf den Benutzercomputer heruntergeladen werden.

Deaktivieren Sie das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP untersuchen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht untersucht, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, bevor die Nachrichten auf den Benutzercomputer heruntergeladen werden. In diesem Fall werden die Nachrichten von der Erweiterung der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, die in den Mail-Client Microsoft Office Outlook integriert ist, wenn das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden** aktiviert ist. Die Untersuchung erfolgt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

> Wenn Sie einen anderen Mail-Client als Microsoft Office Outlook verwenden und das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP untersuchen** deaktiviert ist, werden die Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, nicht von der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht.

- Aktivieren Sie das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**, um den Zugriff auf die Einstellungen für die Komponente „Schutz vor E-Mail-Bedrohungen“ aus dem Programm Microsoft Office Outlook zu ermöglichen und die Untersuchung von Nachrichten zu aktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Untersuchung erfolgt mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und wird ausgeführt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  Deaktivieren Sie das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**, um den Zugriff auf die Einstellungen für die Komponente „Schutz vor E-Mail-Bedrohungen“ aus dem Programm Microsoft Office Outlook zu untersagen und die Untersuchung von Nachrichten zu deaktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Option bezieht sich auf die Untersuchung mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und ausgeführt werden kann, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  > Die Erweiterung für die Komponente “Schutz vor E-Mail-Bedrohungen” wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

6. Speichern Sie die vorgenommenen Änderungen.

Untersuchung zusammengesetzter Dateien, die an E-Mail-Nachrichten angehängt sind

Sie können die Untersuchung von Objekten, die an Nachrichten angehängt sind, aktivieren oder deaktivieren, und für zu untersuchende Objekte, die an Nachrichten angehängt sind, eine maximale Größe und eine maximale Untersuchungsdauer festlegen.

Um die Untersuchung von zusammengesetzten Dateien anzupassen, die an E-Mail-Nachrichten angehängt sind, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Konfigurieren Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** die Untersuchungseinstellungen:

   - **Angehängte Dateien in Microsoft Office-Formaten untersuchen**. Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.

   - **Angehängte Archive untersuchen**. Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.

     Falls Kaspersky Endpoint Security während der Untersuchung im Text der Nachricht ein Kennwort für ein Archiv erkennt, wird dieses Kennwort verwendet, um den Inhalt des Archivs auf bösartige Anwendungen zu untersuchen. Das Kennwort wird in diesem Fall nicht gespeichert. Ein Archiv wird während der Untersuchung entpackt. Wenn während des Entpackungsvorgangs ein Anwendungsfehler auftritt, können Sie die unter dem folgenden Pfad gespeicherten entpackten Dateien manuell löschen: %systemroot%\temp. Diese Dateien besitzen das Präfix PR.

   - **Archive nicht untersuchen, wenn größer als n MB**. Ist das Kontrollkästchen aktiviert, so schließt die Komponente „Schutz vor E-Mail-Bedrohungen“ die Archive, die an E-Mail-Nachrichten angehängt sind, von der Untersuchung aus, falls sie die festgelegte Größe überschreiten. Ist das Kontrollkästchen deaktiviert, so untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die an E-Mail-Nachrichten angehängten Archive unabhängig von deren Größe.

   - **Untersuchungsdauer von Archiven auf n Sekunden beschränken**. Wenn dieses Kontrollkästchen aktiviert ist, wird die Untersuchungsdauer für Archive, die an E-Mail-Nachrichten angehängt sind, auf die festgelegte Dauer beschränkt.

5. Speichern Sie die vorgenommenen Änderungen.

Anlagenfilterung in E-Mail-Nachrichten

Die Funktionalität der Anlagenfilterung wird für ausgehende E-Mail-Nachrichten nicht angewendet.

Schädliche Programme können sich in Form von den Anlagen für E-Mail-Nachrichten verbreiten. Sie können eine Filterung nach dem Typ der Nachrichtenanhänge einrichten, damit Dateien der festgelegten Typen automatisch umbenannt oder gelöscht werden. Durch das Umbenennen bestimmter Typen kann Kaspersky Endpoint Security Ihren Computer vor dem automatischen Start von schädlichen Programmen schützen.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung anzupassen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Führen Sie im Abschnitt **Filter für Anhänge** einen der folgenden Schritte aus:

   - Wählen Sie die Variante **Filter nicht anwenden**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ Nachrichtenanhänge nicht filtert.

- Wählen Sie die Variante **Anlagen der ausgewählten Typen umbenennen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die an Nachrichten angehängten Dateien der angegebenen Typen umbenennt.

- Wählen Sie die Variante **Anhänge der ausgewählten Dateitypen löschen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die an Nachrichten angehängten Dateien der angegebenen Typen löscht.

5. Wenn Sie beim vorherigen Schritt der Anleitung die Variante **Anlagen der ausgewählten Typen umbenennen** oder die Variante **Anlagen der ausgewählten Typen löschen** gewählt haben, aktivieren Sie die Kontrollkästchen für die erforderlichen Dateitypen.

6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Erweiterungen für die Anlagenfilterung

Sie können die Liste der Erweiterungen für Anlagenfilterung in eine XML-Datei exportieren. Mit der Export-/Importfunktion können Sie die Liste der Regeln der Erweiterungen sichern oder die Liste auf einen anderen Server migrieren.

So exportieren und importieren Sie eine Liste von Erweiterungen der Anlagenfilterung in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.
6. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.
7. Wählen Sie im geöffneten Fenster die Registerkarte **Anlagenfilterung**.
8. So exportieren Sie die Liste der Erweiterungen:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Erweiterungen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
9. So importieren Sie die Liste der Erweiterungen:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Erweiterungen möchten.
   c. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Erweiterungen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
10. Speichern Sie die vorgenommenen Änderungen.

[So exportieren und importieren Sie eine Liste von Erweiterungen zur Anlagenfilterung in der Web Console und der Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste von Erweiterungen exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
5. So exportieren Sie die Liste der Erweiterungen im Block **Anlagenfilterung**:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Erweiterungen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
6. So importieren Sie eine Liste von Erweiterungen im Block **Anlagenfilterung**:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Erweiterungen möchten.
   c. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Erweiterungen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

E-Mail-Untersuchung in Microsoft Office Outlook

Bei der Installation von Kaspersky Endpoint Security wird eine Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ in das Programm Microsoft Office Outlook (im Folgenden „Outlook“ genannt) integriert. Sie erlaubt es, aus dem Programm Outlook zu den Einstellungen für die Komponente „Schutz vor E-Mail-Bedrohungen“ zu wechseln und festzulegen, zu welchem Zeitpunkt E-Mail-Nachrichten auf Viren und andere bedrohliche Programme untersucht werden sollen. Die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ kann ein- und ausgehende E-Mail-Nachrichten untersuchen, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Kaspersky Endpoint Security unterstützt auch andere Mail-Clients (z. B. Microsoft Outlook Express®, Windows Mail und Mozilla™ Thunderbird™).

Die „Schutz vor E-Mail-Bedrohungen“-Erweiterung unterstützt Vorgänge mit Outlook 2010, 2013, 2016 und 2019.

Bei der Verwendung des Mail-Clients Mozilla Thunderbird werden Nachrichten, die mit dem IMAP-Protokoll übertragen werden, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht auf Viren und andere bedrohliche Programme untersucht, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

In Outlook werden eingehende E-Mail-Nachrichten zuerst von der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht (sofern auf der Programmoberfläche von Kaspersky Endpoint Security das Kontrollkästchen POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen aktiviert ist). Anschließend werden eingehende E-Mail-Nachrichten von der Outlook-Erweiterung für „Schutz vor E-Mail-Bedrohungen“ gescannt. Findet die Komponente „Schutz vor E-Mail-Bedrohungen“ in einer E-Mail-Nachricht ein schädliches Objekt, so werden Sie darüber informiert.

Die Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“ können direkt in Outlook angepasst werden, wenn die Microsoft Outlook-Erweiterung auf der Programmoberfläche von Kaspersky Endpoint Security aktiviert ist.

Ausgehende Nachrichten werden zuerst von der Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht und anschließend von der Komponente „Schutz vor E-Mail-Bedrohungen“ gescannt.

Wenn die E-Mail-Untersuchung mithilfe der Erweiterung der Komponente „Schutz vor E-Mail-Bedrohungen“ für Outlook erfolgt, wird empfohlen, den Cache-Modus für den Exchange-Server zu verwenden (Use Cached Exchange Mode). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.

Um den Modus der Outlook-Erweiterung für den Schutz vor E-Mail-Bedrohungen mithilfe von Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.
6. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor E-Mail-Bedrohungen** wird geöffnet.
7. Klicken Sie im Abschnitt **Integration ins System** auf **Einstellungen**.
8. Gehen Sie im Fenster **E-Mail-Schutz** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Beim Empfang untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn sie im E-Mail-Postfach eintreffen.
   - Aktivieren Sie das Kontrollkästchen **Beim Lesen untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn der Benutzer sie zum Lesen öffnen möchte.

- Aktivieren Sie das Kontrollkästchen **Beim Senden untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die ausgehenden Nachrichten beim Senden untersucht.

9. Speichern Sie die vorgenommenen Änderungen.

Schutz vor Netzwerkbedrohungen

Die Komponente „Schutz vor Netzwerkbedrohungen“ (IDS, Intrusion Detection System) überwacht den eingehenden Netzwerkverkehr auf Aktivität, die für Netzwerkangriffe typisch ist. Wenn Kaspersky Endpoint Security einen Netzwerkangriff auf den Computer erkennt, sperrt das Programm die Netzwerkverbindung mit dem angreifenden Computer.

Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Die Liste der Netzwerkangriffe, die von der Komponente „Schutz vor Netzwerkbedrohungen“ erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren

Der Schutz vor Netzwerkbedrohungen ist standardmäßig aktiviert und läuft im optimalen Modus. Bei Bedarf können Sie den Schutz vor Netzwerkbedrohungen deaktivieren.

Um den Schutz vor Netzwerkbedrohungen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Schutz vor Netzwerkbedrohungen** aus.
3. Verwenden Sie den Schalter **Schutz vor Netzwerkbedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn der Schutz vor Netzwerkbedrohungen aktiviert ist, durchsucht Kaspersky Endpoint Security eingehenden Netzwerkverkehr nach Aktivitäten, die für Netzwerkangriffe typisch sind. Wenn Kaspersky Endpoint Security einen Netzwerkangriff auf den Computer erkennt, sperrt das Programm die Netzwerkverbindung mit dem angreifenden Computer.

Blockieren eines angreifenden Computers

So blockieren Sie einen angreifenden Computer:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Schutz vor Netzwerkbedrohungen** aus.
3. Aktivieren Sie das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für n Minuten**.

Ist dieses Kontrollkästchen aktiviert, so fügt die Komponente „Schutz vor Netzwerkbedrohungen“ den angreifenden Computer zur Sperrliste hinzu. Das bedeutet, dass die Komponente „Schutz vor Netzwerkbedrohungen“ die Netzwerkverbindung mit dem angreifenden Computer nach dem ersten Netzwerkangriffsversuch für die angegebene Zeitspanne blockiert. Diese Sperre schützt den Computer des Benutzers automatisch vor möglichen zukünftigen Netzwerkangriffen von derselben Adresse aus.

Die Sperrliste können Sie im Fenster Netzwerkmonitor ansehen.

Kaspersky Endpoint Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.

4. Sie können die Zeit, für die ein angreifender Computer blockiert werden soll, im Feld rechts vom Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für n Minuten** ändern.

5. Speichern Sie die vorgenommenen Änderungen.

Wenn Kaspersky Endpoint Security einen versuchten Netzwerkangriff auf den Computer des Benutzers erkennt, blockiert es daher alle Verbindungen mit dem angreifenden Computer.

Adressen anpassen, die bei der Sperrung als Ausnahmen gelten sollen

Kaspersky Endpoint Security kann einen Netzwerkangriff erkennen und eine ungesicherte Netzwerkverbindung blockieren, die eine große Anzahl von Paketen (z. B. von Überwachungskameras) überträgt. Um mit vertrauenswürdigen Geräten zu arbeiten, können Sie die IP-Adressen dieser Geräte zu der Liste der Ausnahmen hinzufügen.

Um Adressen anzupassen, die bei der Sperrung als Ausnahmen gelten sollen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Schutz vor Netzwerkbedrohungen** aus.

3. Klicken Sie auf den Link **Ausnahmen anpassen**.

4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

5. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

6. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen verfolgt Kaspersky Endpoint Security nicht die Aktivität von Geräten auf der Ausnahmenliste.

Exportieren und Importieren der Liste der Ausnahmen von der Sperrung

Sie können die Liste der Ausnahmen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um die Listen der Erweiterungen zu sichern oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor Netzwerkbedrohungen** aus.
6. Klicken Sie im Block **Einstellungen für den Schutz vor Netzwerkbedrohungen** auf die Schaltfläche **Ausnahmen**.
7. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
8. So importieren Sie die Ausnahmeliste:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
9. Speichern Sie die vorgenommenen Änderungen.

[So exportieren und importieren Sie eine Liste der Erweiterungen in der Web Console und der Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste von Erweiterungen exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.
5. Klicken Sie im Block **Einstellungen für den Schutz vor Netzwerkbedrohungen** auf den Link **Ausnahmen**.

   Die Liste der Ausnahmen öffnet sich.
6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.
   d. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   e. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
7. So importieren Sie die Ausnahmeliste:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

Schutz vor Netzwerkangriffen nach Typ konfigurieren

Mit Kaspersky Endpoint Security können Sie den Schutz vor den folgenden Arten von Netzwerkangriffen verwalten:

- *Network Flooding* ist ein Angriff auf die Netzwerkressourcen einer Organisation (z. B. auf einen Webserver). Bei diesem Angriff wird eine große Anzahl von Anforderungen gesendet, was die Bandbreite der Netzwerkressourcen überlastet. In einem solchen Fall können Benutzer nicht auf die Netzwerkressourcen der Organisation zugreifen.

- Beim Angriff *Port Scanning* werden die UDP-Ports, TCP-Ports und Netzwerkdienste des Computers gescannt. Bei diesem Angriff können Angreifer ermitteln, wie anfällig der Computer für Angriffe ist, bevor sie gefährlichere Arten von Netzwerkangriffen starten. Mithilfe von Port Scanning können Angreifer außerdem das Betriebssystem des Computers identifizieren und die entsprechenden Netzwerkangriffe für dieses Betriebssystem auswählen.

- Bei einem Angriff vom Typ *MAC-Spoofing* wird die MAC-Adresse eines Netzwerkgeräts (einer Netzwerkkarte) verändert. Dann kann der Angreifer die Daten, die an das Gerät gesendet werden, auf ein anderes Gerät umleiten und auf diese Daten zugreifen. Kaspersky Endpoint Security kann Mac-Spoofing-Angriffe blockieren und solche Angriffe melden

Sie können die Erkennung dieser Angriffstypen deaktivieren, falls einige Ihrer zulässigen Programme Vorgänge ausführen, die für diese Angriffstypen typisch sind. Auf diese Weise können Fehlalarme vermieden werden.

Standardmäßig überwacht Kaspersky Endpoint Security keine Angriffe vom Typ „Network Flooding“, „Port Scanning“ und „MAC-Spoofing“.

So konfigurieren Sie den Schutz vor Netzwerkangriffen nach Typ:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Schutz vor Netzwerkbedrohungen** aus.

3. Verwenden Sie den Schalter **Port Scanning und Network Flooding als Angriff einstufen**, um die Erkennung dieser Angriffe zu aktivieren oder zu deaktivieren.

4. Verwenden Sie den Schalter **MAC-Spoofing-Schutz**.

5. Wählen Sie im Block **Wenn ein MAC-Spoofing-Angriff erkannt wird** eine der folgenden Optionen aus:

   - **Nur melden**.

   - **Melden und blockieren**.

6. Speichern Sie die vorgenommenen Änderungen.

Firewall

Die „Firewall“ blockiert nicht autorisierte Verbindungen mit dem Computer, wenn das Internet oder ein lokales Netzwerk verwendet wird. Die „Firewall“ kontrolliert auch die Netzwerkaktivität der Programme auf dem Computer. Dadurch wird das lokales Unternehmensnetzwerk vor dem Diebstahl persönlicher Daten und anderen Angriffen geschützt. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der *vordefinierten Netzwerkregeln*.

Der Administrationsagent wird für die Interaktion mit Kaspersky Security Center verwendet. Die Firewall erstellt automatisch Netzwerkregeln, die für die ordnungsgemäße Funktion des Programms und des Administrationsagenten erforderlich sind. Dadurch bedingt öffnet die Firewall bestimmte Ports auf dem Computer. Welche Ports geöffnet werden, hängt von der Rolle des Computers ab (z. B. Verteilungspunkt). Weitere Informationen zu den Ports, die auf dem Computer geöffnet werden, finden Sie in der *Hilfe zu Kaspersky Security Center*.

Netzwerkregeln

Sie können die Netzwerkregeln auf folgenden Ebenen anpassen:

- *Regeln für Netzwerkpakete*. Sie dienen zur Definition von Beschränkungen für die Netzwerkpakete, wobei das Programm keine Rolle spielt. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Kaspersky Endpoint Security hat vordefinierte Netzwerkregeln für Pakete mit Lösungen, die von den Kaspersky-Experten empfohlen werden.

- *Netzwerkregeln für das Programm*. Sie dienen zur Definition von Beschränkungen der Netzwerkaktivität eines konkreten Programms. Dabei werden nicht nur die Merkmale des Netzwerkpakets berücksichtigt, sondern auch das konkrete Programm, an das dieses Netzwerkpaket adressiert ist oder welches das Senden dieses Netzwerkpakets initiiert hat.

Die Komponente „Programm-Überwachung" kontrolliert mithilfe von *Programmrechten* den Zugriff auf Betriebssystemressourcen, Prozesse und persönliche Daten.

Wenn ein Programm zum ersten Mal gestartet wird, führt die „Firewall" folgende Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.

2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Firewall" zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Das Programm wird einer *Sicherheitsgruppe* zugewiesen: Vertrauenswürdig, Schwach beschränkt, Stark beschränkt, Nicht vertrauenswürdig.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall" und „Programm-Überwachung" zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall" oder nur für die „Programm-Überwachung" zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung" aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Netzwerkaktivität des Programms. Für Programme aus der Sicherheitsgruppe „Stark beschränkt" sind beispielsweise alle Netzwerkverbindungen verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde das Programm nicht verändert, so wendet die Komponente die aktuellen Netzwerkregeln darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Prioritäten der Netzwerkregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Netzwerkaktivität in mehreren Regeln vorkommt, reguliert die „Firewall“ die Netzwerkaktivität nach der Regel mit der höchsten Priorität.

Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme. Sind für eine Art der Netzwerkaktivität gleichzeitig Netzwerkregeln für Pakete und Netzwerkregeln für Programme vorhanden, wird diese Netzwerkaktivität nach den Netzwerkregeln für Pakete verarbeitet.

Netzwerkregeln für Programme funktionieren wie folgt: Eine Netzwerkregel für Programme enthält Zugriffsregeln je nach Netzwerkstatus: *öffentlich*, *lokal*, *vertrauenswürdig*. Zum Beispiel ist für die Sicherheitsgruppe „Stark beschränkt“ standardmäßig jede Netzwerkaktivität eines Programms in Netzwerken mit beliebigem Status verboten. Wenn für ein bestimmtes Programm (übergeordnetes Programm) eine Netzwerkregel vorliegt, werden die untergeordneten Prozesse anderer Programme gemäß der Netzwerkregel des übergeordneten Programms ausgeführt. Gibt es keine Netzwerkregel für ein Programm, so werden die untergeordneten Prozesse gemäß der Regel für den Zugriff auf Netzwerke der Sicherheitsgruppe des Programms ausgeführt.

Beispiel: Sie haben jede Netzwerkaktivität aller Programme für Netzwerke mit beliebigem Status verboten, unter Ausnahme von Browser X. Wenn Browser X (übergeordnetes Programm) die Installation von Browser Y startet (untergeordneter Prozess), erhält Browser Y Zugriff auf das Netzwerk und lädt die erforderlichen Dateien herunter. Nach der Installation sind für Browser Y alle Netzwerkverbindungen verboten, wobei die Einstellungen der Firewall gelten. Um dem Installationsprogramm von Browser Y die Netzwerkaktivität als untergeordneter Prozess zu verbieten, muss eine Netzwerkregel für das Installationsprogramm von Browser Y hinzugefügt werden.

Statusvarianten der Netzwerkverbindungen

Bei der Kontrolle der Netzwerkaktivität kann die „Firewall“ den Status einer Netzwerkverbindung berücksichtigen. Den Status der Netzwerkverbindung erhält Kaspersky Endpoint Security vom Betriebssystem des Computers. Den Status einer Netzwerkverbindung im Betriebssystem legt der Benutzer beim Einrichten der Verbindung fest. Sie können den Status der Netzwerkverbindung in den Einstellungen von Kaspersky Endpoint Security ändern. Dann kontrolliert die „Firewall“ die Netzwerkaktivität anhand des Netzwerkstatus aus den Einstellungen von Kaspersky Endpoint Security, nicht anhand des Status aus dem Betriebssystem.

Für eine Netzwerkverbindung sind folgende Statusvarianten vorgesehen:

- **Öffentliches Netzwerk**. Das Netzwerk wird durch Antiviren-Programme, Firewalls oder Filter geschützt (z. b. WLAN in einem Café). Für den Benutzer eines Computers, der mit einem solchen Netzwerk verbunden ist, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Auch Drittnutzer erhalten über gemeinsame Ordner oder Fernzugriff keinen Zugang zu Informationen auf dem Desktop Ihres Computers. Die Firewall filtert die Netzwerkaktivität für jedes Programm nach den für dieses Programm vorhandenen Netzwerkregeln.

  Das Internet erhält von der Firewall standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.

- **Lokales Netzwerk**. Netzwerk für Benutzer, für die der Zugriff auf die Dateien und Drucker dieses Computers beschränkt ist (beispielsweise ein lokales Unternehmensnetzwerk oder ein privates Netzwerk).

- **Vertrauenswürdiges Netzwerk**. Sicheres Netzwerk, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen. Für Netzwerke mit diesem Status erlaubt die Firewall im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.

Firewall aktivieren und deaktivieren

Die Firewall ist standardmäßig aktiviert und arbeitet im optimalen Modus.

Um die Firewall zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Verwenden Sie den Schalter **Firewall**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Status einer Netzwerkverbindung ändern

Das Internet erhält von der Firewall standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Verfügbare Netzwerke**.
4. Wählen Sie die Netzwerkverbindung, deren Status Sie ändern möchten.
5. Wählen Sie in der Spalte **Netzwerktyp** den Status der Netzwerkverbindung aus:
   - **Öffentliches Netzwerk**. Das Netzwerk wird durch Antiviren-Programme, Firewalls oder Filter geschützt (z. b. WLAN in einem Café). Für den Benutzer eines Computers, der mit einem solchen Netzwerk verbunden ist, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Auch Drittnutzer erhalten über gemeinsame Ordner oder Fernzugriff keinen Zugang zu Informationen auf dem Desktop Ihres Computers. Die Firewall filtert die Netzwerkaktivität für jedes Programm nach den für dieses Programm vorhandenen Netzwerkregeln.
   - **Lokales Netzwerk**. Netzwerk für Benutzer, für die der Zugriff auf die Dateien und Drucker dieses Computers beschränkt ist (beispielsweise ein lokales Unternehmensnetzwerk oder ein privates Netzwerk).
   - **Vertrauenswürdiges Netzwerk**. Sicheres Netzwerk, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen. Für Netzwerke mit diesem Status erlaubt die Firewall im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.
6. Speichern Sie die vorgenommenen Änderungen.

Arbeit mit Netzwerkregeln für Pakete

Bei der Arbeit mit Netzwerkregeln für Pakete können Sie folgende Aktionen ausführen:

- Erstellen einer neuen Netzwerkregel für Pakete

  Sie können eine neue Netzwerkregel für Pakete erstellen. Dazu wird eine Kombination von Bedingungen und Aktionen für Netzwerkpakete und Datenströme festgelegt.

- Aktivieren und Deaktivieren einer Netzwerkregel für Pakete

  Alle Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt werden, besitzen den Status *Aktiv*. Ist eine Netzwerkregel für Pakete aktiviert, wendet die Firewall diese Regel an.

  Sie können eine beliebige Netzwerkregel für Pakete deaktivieren, die auf der Liste der Netzwerkregeln für Pakete steht. Ist eine Netzwerkregel für Pakete deaktiviert, wird diese Regel vorübergehend nicht von der Firewall verwendet.

  Eine neue Netzwerkregel für Pakete, die vom Benutzer erstellt wurde, wird standardmäßig mit dem Status *Aktiv* zur Liste Netzwerkregeln für Pakete hinzugefügt.

- Ändern der Einstellungen einer vorhandenen Netzwerkregel für Pakete

  Nach Erstellung einer neuen Netzwerkregel für Pakete können Sie ihre Einstellungen jederzeit ändern.

- Ändern der Firewall-Aktion für eine Netzwerkregel für Pakete

  In der Liste der Netzwerkregeln für Pakete können Sie die Aktion ändern, die von der Firewall ausgeführt wird, wenn eine Netzwerkaktivität erkannt wird, die der angegebenen Netzwerkregel für Pakete entspricht.

- Ändern der Priorität einer Netzwerkregel für Pakete

  Sie können die Priorität einer in der Liste markierten Netzwerkregel für Pakete ändern.

- Löschen einer Netzwerkregel für Pakete

  Sie können eine Netzwerkregel für Pakete löschen, wenn Sie nicht möchten, dass diese Regel beim Fund einer Netzwerkaktivität von der Firewall angewendet wird und dass die Regel mit dem Status *Deaktiviert* in der Liste der Netzwerkregeln für Pakete erscheint.

Eine Netzwerkpaketregel erstellen

Eine Netzwerkpaketregel kann auf folgende Arten erstellt werden:

- Verwenden Sie das Tool Netzwerkmonitor.

  Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen. Das ist praktisch, da Sie so nicht alle Regeleinstellungen konfigurieren müssen. Einige Firewall-Einstellungen werden automatisch aus den Daten des Netzwerkmonitors eingefügt. Der Netzwerkmonitor ist nur in der Programmoberfläche verfügbar.

- Konfigurieren Sie die Firewall-Einstellungen.

  Auf diese Weise können Sie die einzelnen Firewall-Einstellungen flexibel anpassen. Sie können Regeln für jede Netzwerkaktivität erstellen, selbst wenn derzeit keine Netzwerkaktivität vorhanden ist.

Bei der Erstellung von Regeln für Netzwerkpakete ist zu beachten, dass diesen Vorrang vor den Netzwerkregeln für Programme eingeräumt wird.

Verwendung des Netzwerkmonitors zum Erstellen einer Netzwerkpaketregel in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen → Netzwerkmonitor**.
2. Wählen Sie die Registerkarte **Netzwerkaktivität** aus.

   Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt.
3. Wählen Sie im Kontextmenü einer Netzwerkverbindung den Punkt **Paketregel erstellen** aus.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
4. Setzen Sie den Status **Aktiv** für die Paketregel.
5. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
6. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
7. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
8. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.
9. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
10. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Firewall-Einstellungen zum Erstellen einer Netzwerkpaketregel in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf die Schaltfläche **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
4. Klicken Sie auf **Hinzufügen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
5. Setzen Sie den Status **Aktiv** für die Paketregel.
6. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
7. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
8. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
9. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.
10. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
11. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkpaketregel in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall** aus.
6. Klicken Sie im Block **Firewall-Einstellungen** auf die Schaltfläche **Einstellungen**.

   Eine Liste mit Netzwerkpaketregeln und eine Liste mit Netzwerkregeln für Programme werden geöffnet.
7. Wählen Sie die Registerkarte **Regeln für Netzwerkpakete** aus.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
8. Klicken Sie auf **Hinzufügen**.

   Dadurch werden die Paketregel-Eigenschaften geöffnet.
9. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
10. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

    Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf die Schaltfläche klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

    Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
11. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
12. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.
13. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
14. Speichern Sie die vorgenommenen Änderungen.

Die Firewall wird Netzwerkpakete gemäß dieser Regel überwachen. Eine Paketregel kann in der Firewall deaktiviert werden, ohne dass sie aus der Liste gelöscht werden muss. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

So erstellen Sie eine Netzwerkpaketregel in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz** → **Firewall** aus.
5. Klicken Sie im Block **Firewall-Einstellungen** auf den Link **Regeln für Netzwerkpakete**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
6. Klicken Sie auf **Hinzufügen**.

   Dadurch werden die Paketregel-Eigenschaften geöffnet.
7. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
8. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage auswählen** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
9. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
10. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.
11. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
12. Speichern Sie die vorgenommenen Änderungen.

Die Firewall wird Netzwerkpakete gemäß dieser Regel überwachen. Eine Paketregel kann in der Firewall deaktiviert werden, ohne dass sie aus der Liste gelöscht werden muss. Verwenden Sie den Schalter in der Spalte **Status**, um die Paketregel zu aktivieren oder zu deaktivieren.

Einstellungen der Netzwerkpaketregel

Einstellung	Beschreibung
Aktion	**Erlauben**. **Blockieren** **Nach Regeln für Programme**. Bei Auswahl dieser Variante wendet die Firewall die Netzwerkregeln des Programms auf die Netzwerkverbindung an.
Protokoll	Überwachen Sie die Netzwerkaktivität über das ausgewählte Protokoll: TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen. Wurde TCP oder UDP als Protokoll gewählt, können Sie kommagetrennt die Portnummern des Benutzercomputers und des Remote-Computers angeben, zwischen denen die Verbindung überwacht werden soll.

Richtung	**Eingehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle eingehenden Netzwerkpakete an. **Eingehend** Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine von einem Remote-Computer initiierte Verbindung gesendet werden. **Eingehend / Ausgehend**. Die Firewall wendet diese Netzwerkregel sowohl auf eingehende als auch auf ausgehende Netzwerkpakete an. Dabei bleibt unberücksichtigt, ob die Netzwerkverbindung vom lokalen Computer oder von einem Remote-Computer initiiert wurde. **Ausgehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle ausgehenden Netzwerkpakete an. **Ausgehend** Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine vom Benutzercomputer initiierte Verbindung gesendet werden. Das TCP-Protokoll stellt eine Verbindung her. Verwenden Sie für TCP die Richtungen **Eingehend**, **Ausgehend** und **Eingehend/Ausgehend**. Alle anderen Protokolle stellen keine Verbindungen her, senden aber Pakete. Verwenden Sie für alle anderen Protokolle die Richtungen **Eingehend (Paket)**, **Ausgehend (Pakete)** oder **Eingehend/Ausgehend**.
Netzwerkadapter	Netzwerkadapter, die Netzwerkpakete senden und/oder empfangen können. Das Festlegen der Einstellungen für Netzwerkadapter erlaubt das Unterscheiden von Netzwerkpaketen, die von den Netzwerkadaptern mit denselben IP-Adressen gesendet oder empfangen wurden.
Lebensdauer (TTL)	Beschränken Sie die Überwachung von Netzwerkpaketen basierend auf ihrer Lebensdauer (TTL).
Remote-Adressen	Netzwerkadressen der Remote-Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegebenen Bereich von Remote-Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen oder ein untergeordnetes Netzwerk auswählen (Vertrauenswürdige Netzwerke, Lokale Netzwerke, Öffentliche Netzwerke).
Lokale Adressen	Netzwerkadressen der Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegeben Bereich von lokalen Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen oder eine separate Liste mit IP-Adressen erstellen. Es ist für Anwendungen nicht immer möglich, die lokale Adresse zu bekommen. In diesem Fall wird diese Einstellung ignoriert.

Netzwerkregel für Pakete aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um eine Regel für Netzwerkpakete zu aktivieren oder zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf die Schaltfläche **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie in der Liste die erforderliche Regel für Netzwerkpakete.

5. Verwenden Sie den Schalter in der Spalte **Status**, um die Regel zu aktivieren oder zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

Verhalten der Firewall in Bezug auf Netzwerkregeln für Pakete ändern

Gehen Sie folgendermaßen vor, um die Firewall-Aktion für die Regel für Netzwerkpakete zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf die Schaltfläche **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie aus der Liste der Netzwerkregeln für Pakete eine Regel und klicken Sie auf **Ändern**, um sie zu ändern.

5. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, welche die Firewall bei Erkennen der entsprechenden Art von Netzwerkaktivität ausführen soll:

   - **Erlauben**.
   - **Blockieren**
   - **Nach Regeln für Programme**.

6. Speichern Sie die vorgenommenen Änderungen.

Priorität einer Netzwerkregel für Pakete ändern

Die Ausführungspriorität einer Regel für Netzwerkpakete wird durch ihre Position in der Liste der Regeln für Netzwerkpakete bestimmt. Die Netzwerkregel, die in der Liste der Regeln für Netzwerkpakete an erster Stelle steht, besitzt die höchste Priorität.

Jede Regel für Netzwerkpakete, die Sie manuell erstellen, wird am Ende der Liste der Regeln für Netzwerkpakete hinzugefügt und besitzt die niedrigste Priorität.

Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Regeln für Netzwerkpakete stehen (von oben nach unten). Entsprechend jeder Regel für Netzwerkpakete, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Gehen Sie folgendermaßen vor, um die Priorität einer Regel für Netzwerkpakete zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf die Schaltfläche **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.
4. Wählen Sie in der Liste die Regel für Netzwerkpakete, deren Priorität Sie ändern möchten.
5. Verwenden Sie die Schaltflächen **Aufwärts** und **Abwärts**, um die Netzwerkregel für Pakete an die entsprechende Position in der Liste der Regeln für Netzwerkpakete zu verschieben.
6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Netzwerkpaketregeln

Sie können die Liste der Regeln für Netzwerkpakete in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie die Liste der Regeln für Netzwerkpakete sichern oder die Liste auf einen anderen Server migrieren.

Exportieren und Importieren einer Liste von Regeln für Netzwerkpakete in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall** aus.
6. So exportieren Sie die Liste der Regeln für Netzwerkpakete:
   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
7. So importieren Sie eine Liste der Regeln für Netzwerkpakete:
   a. Klicken Sie auf **Import**.
      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

[So exportieren und importieren Sie eine Liste von Regeln für Netzwerkpakete in der Web Console und der Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste der Regeln exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz** → **Firewall** aus.
5. Klicken Sie auf **Regeln für Netzwerkpakete**.
6. So exportieren Sie die Liste der Regeln für Netzwerkpakete:
   a. Wählen Sie die Regeln, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Regeln exportieren möchten, oder exportieren Sie die gesamte Liste.
   d. Klicken Sie auf **Export**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine XML-Datei im Standard-Download-Ordner.
7. So importieren Sie eine Liste der Regeln für Netzwerkpakete:
   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

Verwendung von Netzwerkregeln für Programme

Kaspersky Endpoint Security ordnet standardmäßig alle Programme, die auf dem Benutzercomputer installiert sind, nach dem Herstellernamen der Programme an, deren Datei- und Netzwerkaktivität kontrolliert wird. Programmgruppen werden nach Sicherheitsgruppen angeordnet. Alle Programme und Programmgruppen erben folgende Eigenschaften der jeweiligen übergeordneten Gruppe: Kontrollregeln für Programme, Netzwerkregeln für das Programm, sowie Ausführungspriorität.

Die Komponenten Programm-Überwachung und Firewall verwenden standardmäßig die Netzwerkregeln für eine Programmgruppe zur Filterung der Netzwerkaktivität aller Programme dieser Gruppe. Die Netzwerkregeln für eine Programmgruppe legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerkverbindungen besitzen.

Die Firewall erstellt standardmäßig eine Auswahl von Netzwerkregeln für jede Gruppe von Programmen, die von Kaspersky Endpoint Security auf dem Computer gefunden wurden. Sie können die Firewall-Aktion für die standardmäßig erstellten Netzwerkregeln für eine Programmgruppe ändern. Standardmäßig erstellte Netzwerkregeln für eine Programmgruppe können nicht geändert, gelöscht oder deaktiviert werden. Außerdem ist ihre Priorität unveränderlich.

Sie können eine Netzwerkregel für ein bestimmtes Programm erstellen. Eine solche Regel besitzt eine höhere Priorität als die Netzwerkregel der Gruppe, zu welcher dieses Programm gehört.

Eine Netzwerkregel für das Programm erstellen

Standardmäßig erfolgt die Aktivitätskontrolle für Programme mittels Netzwerkregeln. Diese Regeln werden für die Sicherheitsgruppe angelegt, in die das Programm bei seinem ersten Start von Kaspersky Endpoint Security verschoben wurde. Bei Bedarf können Sie Netzwerkregeln für eine gesamte Sicherheitsgruppe, für ein einzelnes Programm oder für eine Programmgruppe innerhalb einer Sicherheitsgruppe erstellen.

Manuell angelegte Netzwerkregeln haben eine höhere Priorität als Netzwerkregeln, die für eine Sicherheitsgruppe festgelegt wurden. Mit anderen Worten: Wenn manuell angelegte Programmregeln sich von den für die Sicherheitsgruppe festgelegten Programmregeln unterscheiden, überwacht die Firewall die Programmaktivität gemäß den manuell angelegten Programmregeln.

Standardmäßig erstellt die Firewall für jedes Programm die folgenden Netzwerkregeln:

- Jede Netzwerkaktivität in vertrauenswürdigen Netzwerken
- Jede Netzwerkaktivität in lokalen Netzwerken
- Jede Netzwerkaktivität in öffentlichen Netzwerken

Kaspersky Endpoint Security überwacht die Netzwerkaktivität von Programmen wie folgt gemäß vordefinierten Netzwerkregeln:

- „Vertrauenswürdig“ und „Schwach beschränkt“: Alle Netzwerkaktivitäten sind zulässig.
- „Stark beschränkt“ und „Nicht vertrauenswürdig“: Alle Netzwerkaktivitäten sind blockiert.

Vordefinierte Programmregeln können nicht bearbeitet oder gelöscht werden.

Eine Netzwerkregel für das Programm kann auf folgende Arten erstellt werden:

- Verwenden Sie das Tool Netzwerkmonitor.

  Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen. Das ist praktisch, da Sie so nicht alle Regeleinstellungen konfigurieren müssen. Einige Firewall-Einstellungen werden automatisch aus den Daten des Netzwerkmonitors eingefügt. Der Netzwerkmonitor ist nur in der Programmoberfläche verfügbar.

- Konfigurieren Sie die Firewall-Einstellungen.

  Auf diese Weise können Sie die einzelnen Firewall-Einstellungen flexibel anpassen. Sie können Regeln für jede Netzwerkaktivität erstellen, selbst wenn derzeit keine Netzwerkaktivität vorhanden ist.

Beachten Sie beim Erstellen von Netzwerkregeln für Programme, dass Netzwerkpaketregeln Vorrang vor Netzwerkregeln für Programme haben.

Verwendung des Netzwerkmonitors zum Erstellen einer Netzwerkregeln für Programme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Netzwerkmonitor**.
2. Wählen Sie die Registerkarte **Netzwerkaktivität** oder **Offene Ports** aus.

   Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt.

   Auf der Registerkarte **Offene Ports** sind alle geöffneten Ports des Computers aufgelistet.
3. Wählen Sie im Kontextmenü einer Netzwerkverbindung den Punkt **Programmregel erstellen** aus.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
4. Wählen Sie die Registerkarte **Netzwerkregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
5. Klicken Sie auf **Hinzufügen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
6. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
7. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
8. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
9. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.
10. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
11. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Firewall-Einstellungen zum Erstellen einer Netzwerkregeln für Programme in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel erstellt werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
6. Wählen Sie die Registerkarte **Netzwerkregeln**.
7. Klicken Sie auf **Hinzufügen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
8. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
9. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
10. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
11. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.
12. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
13. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkregel für Programme in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall** aus.
6. Klicken Sie im Block **Firewall-Einstellungen** auf die Schaltfläche **Einstellungen**.

   Eine Liste mit Netzwerkpaketregeln und eine Liste mit Netzwerkregeln für Programme werden geöffnet.
7. Wählen Sie die Registerkarte **Netzwerkregeln für Programme** aus.
8. Klicken Sie auf **Hinzufügen**.
9. Geben Sie im folgenden Fenster die Suchkriterien für das Programm ein, für das eine Netzwerkregel erstellt werden soll.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen * und ? bei der Eingabe einer Maske.
10. Klicken Sie auf **Aktualisieren**.

    Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.
11. Wählen Sie das erforderliche Programm.
12. Wählen Sie in der Dropdown-Liste **Ausgewählte Programme zu <Sicherheitsgruppe> hinzufügen** den Punkt **Standardgruppen** aus und klicken Sie auf **OK**.

    Das Programm wird der Standardgruppe hinzugefügt.
13. Wählen Sie das gewünschte Programm aus und klicken Sie dann auf **Rechte für Programme** im Kontextmenü des Programms.

    Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
14. Wählen Sie die Registerkarte **Netzwerkregeln**.

    Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
15. Klicken Sie auf **Hinzufügen**.

    Die Eigenschaften von Netzwerkregeln werden geöffnet.
16. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
17. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

    Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf die Schaltfläche klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

    Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

18. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

19. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.

20. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

21. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkregel für Programme in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Basisschutz** → **Firewall** aus.
5. Klicken Sie im Block **Firewall-Einstellungen** auf den Link **Netzwerkregeln für Programme**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Wählen Sie die Registerkarte **Rechte für Programme** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.
8. Klicken Sie auf den Link **Ausgewählte Zielgruppe**, um die gewünschte Sicherheitsgruppe für das Programm auszuwählen.
9. Wählen Sie den **Programm**typ aus. Klicken Sie auf **Weiter**.

   Wenn Sie eine Netzwerkregel für mehrere Programme erstellen möchten, wählen Sie den Typ der **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.
10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, für die eine Netzwerkregel erstellt werden soll.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
11. Schließen Sie den Assistenten mit einem Klick auf **OK** ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.
12. Klicken Sie im linken Fensterbereich auf das gewünschte Programm.
13. Wählen Sie im rechten Bereich des Fensters den Punkt **Netzwerkregeln** aus der Dropdown-Liste aus.

    Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
14. Klicken Sie auf **Hinzufügen**.

    Die Eigenschaften von Programmregeln werden geöffnet.
15. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
16. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

    Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage auswählen** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

    Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

17. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
18. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.
19. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
20. Speichern Sie die vorgenommenen Änderungen.

Einstellungen der Netzwerkregel für Programme

Einstellung	Beschreibung
Aktion	**Erlauben**. **Blockieren**
Protokoll	Überwachen Sie die Netzwerkaktivität über das ausgewählte Protokoll: TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen. Wurde TCP oder UDP als Protokoll gewählt, können Sie kommagetrennt die Portnummern des Benutzercomputers und des Remote-Computers angeben, zwischen denen die Verbindung überwacht werden soll.
Richtung	**Eingehend** **Eingehend / Ausgehend**. **Ausgehend**
Remote-Adressen	Netzwerkadressen der Remote-Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegebenen Bereich von Remote-Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen oder ein untergeordnetes Netzwerk auswählen (Vertrauenswürdige Netzwerke, Lokale Netzwerke, Öffentliche Netzwerke).
Lokale Adressen	Netzwerkadressen der Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegeben Bereich von lokalen Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen oder eine separate Liste mit IP-Adressen erstellen. Es ist für Anwendungen nicht immer möglich, die lokale Adresse zu bekommen. In diesem Fall wird diese Einstellung ignoriert.

Netzwerkregel für Programme aktivieren und deaktivieren

Um eine Netzwerkregel für Programme zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

Dies öffnet die Liste der Regeln für Programme.

4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel erstellt oder geändert werden soll.

5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.

6. Wählen Sie die Registerkarte **Netzwerkregeln**.

7. Wählen Sie in der Liste der Netzwerkregeln dieser Gruppe die entsprechende Netzwerkregel.

   Das Fenster mit den Eigenschaften für Netzwerkregeln wird geöffnet.

8. Legen Sie den Status **Aktiv** oder **Inaktiv** für die Netzwerkregel fest.

   Sie können eine Netzwerkregel für Programmgruppen nicht deaktivieren, wenn sie standardmäßig von der Firewall erstellt wurde.

9. Speichern Sie die vorgenommenen Änderungen.

Firewall-Aktion für die Netzwerkregel für Programme ändern

Sie können die Firewall-Aktion für alle standardmäßig erstellten Netzwerkregeln eines Programms oder einer Programmgruppe ändern, und Sie können die Firewall-Aktion für eine bestimmte manuell erstellte Netzwerkregel eines Programms oder einer Programmgruppe ändern.

Um die Firewall-Aktion für alle Netzwerkregeln eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.

4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, wenn Sie die Firewall-Aktion für alle entsprechenden standardmäßig erstellten Netzwerkregeln ändern möchten. Manuell erstellte Netzwerkregeln bleiben unverändert.

5. Klicken Sie mit der rechten Maustaste, um das Kontextmenü zu öffnen, wählen Sie **Netzwerkregeln** und dann die Aktion, die Sie zuordnen möchten:

   - **Erben**.
   - **Erlauben**.
   - **Blockieren**

6. Speichern Sie die vorgenommenen Änderungen.

Um die Firewall-Aktion für eine Netzwerkregel eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.
4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, für welche die Aktion einer Netzwerkregel geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
6. Wählen Sie die Registerkarte **Netzwerkregeln**.
7. Wählen Sie die Netzwerkregel, für welche Sie die Firewall-Aktion ändern möchten.
8. Klicken Sie mit der rechten Maustaste auf die Spalte **Erlaubnis** und wählen Sie die gewünschte Aktion:
   - **Erben.**
   - **Erlauben**.
   - **Blockieren**
   - **Protokollieren**.
9. Speichern Sie die vorgenommenen Änderungen.

Priorität der Netzwerkregel für Programme ändern

Die Ausführungspriorität einer Netzwerkregel wird durch ihre Position in der Liste der Netzwerkregeln bestimmt. Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln stehen (von oben nach unten). Entsprechend jeder Netzwerkregel, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Manuell erstellte Netzwerkregeln besitzen eine höhere Priorität als standardmäßig erstellte Netzwerkregeln.

Sie können die Priorität von manuell erstellten Netzwerkregeln für Programmgruppen nicht ändern.

Um die Priorität einer Netzwerkregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.

4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für welche die Priorität der Netzwerkregel geändert werden soll.

5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.

6. Wählen Sie die Registerkarte **Netzwerkregeln**.

7. Wählen Sie die Netzwerkregel, deren Priorität Sie ändern möchten.

8. Verwenden Sie die Schaltflächen **Aufwärts** und **Abwärts**, um die Netzwerkregel an die entsprechende Position in der Liste der Netzwerkregeln zu verschieben.

9. Speichern Sie die vorgenommenen Änderungen.

Netzwerkmonitor

Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen.

Gehen Sie folgendermaßen vor, um den Netzwerkmonitor zu starten:

Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Netzwerkmonitor**.

Das Fenster **Netzwerkmonitor** öffnet sich. Dieses Fenster bietet vier Registerkarten mit Informationen zu den Netzwerkaktivitäten des Benutzercomputers:

- Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt. Auf dieser Registerkarte können Sie auch Netzwerkpaketregeln für den Firewall-Betrieb erstellen.

- Auf der Registerkarte **Offene Ports** sind alle geöffneten Ports des Computers aufgelistet. Auf dieser Registerkarte können Sie auch Netzwerkpaketregeln und Programmregeln für den Firewall-Betrieb erstellen.

- Auf der Registerkarte **Netzwerkverkehr** wird das Volumen des ein- und ausgehenden Netzwerkverkehrs zwischen dem lokalen Computer und anderen Computern des Netzwerks angezeigt, in dem der Computer momentan arbeitet.

- Auf der Registerkarte **Blockierte Computer** sind die IP-Adressen jener Remote-Computern aufgelistet, von deren IP-Adresse ein versuchter Netzwerkangriff erkannt wurde und deren Netzwerkaktivität deshalb von der Komponente „Schutz vor Netzwerkbedrohungen“ blockiert wurde.

Schutz vor modifizierten USB-Geräten

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird. Infolgedessen kann der Virus unter Ihrem Benutzerkonto Befehle ausführen, um z. B. Malware herunterzuladen.

Die Komponente „Schutz vor modifizierten USB-Geräten“ verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.

Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (falls diese verfügbar ist) einen vom Programm generierten digitalen Code einzugeben (siehe nachstehende Abbildung). Dieser Vorgang heißt Autorisierung der Tastatur.

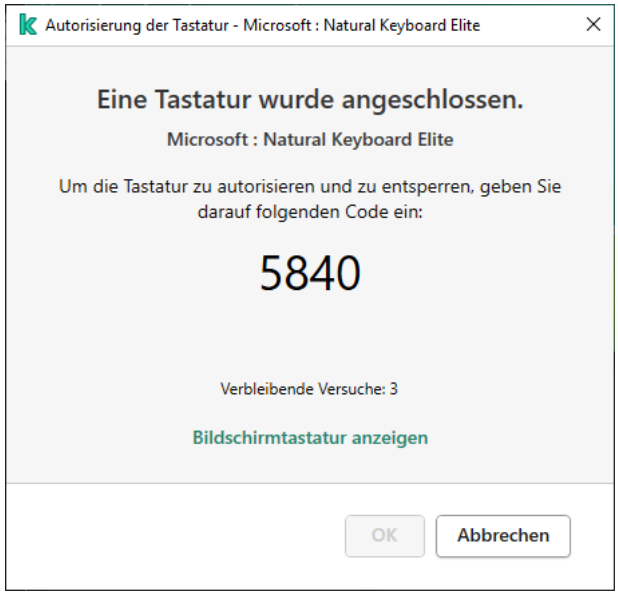
Wurde der richtige Code eingegeben, so speichert das Programm die Identifikationsparameter (VID/PID der Tastatur und Nummer des Ports, über den die Tastatur verbunden ist) in der Liste der autorisierten Tastaturen. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, ist keine Autorisierung erforderlich.

Wenn eine autorisierte Tastatur über einen anderen USB-Port mit dem Computer verbunden wird, fragt das Programm erneut nach der Autorisierung.

Wurde der digitale Code falsch eingegeben, so generiert das Programm einen neuen Code. Die Anzahl der Eingabeversuche für den digitalen Code ist auf drei beschränkt. Nachdem der digitale Code dreimal falsch eingegeben wurde oder das Fenster **Autorisierung der Tastatur <Name der Tastatur>** geschlossen wurde, blockiert das Programm die Eingabe von dieser Tastatur. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, schlägt das Programm erneut vor, die Autorisierung vorzunehmen.

Das Programm erlaubt die Verwendung einer autorisierten Tastatur. Eine Tastatur, die nicht autorisiert wurde, wird blockiert.

Die Komponente „Schutz vor modifizierten USB-Geräten“ wird nicht standardmäßig installiert. Wenn Sie die Komponente „Schutz vor modifizierten USB-Geräten“ benötigen, können Sie die Komponente entweder vor der Programminstallation in den Eigenschaften des Installationspakets hinzufügen oder nach der Programminstallation die Auswahl der Programmkomponenten ändern.



Autorisierung der Tastatur

Schutz vor modifizierten USB-Geräten aktivieren und deaktivieren

USB-Geräte, die vom Betriebssystem als Tastatur erkannt wurden und vor der Installation der Komponente „Schutz vor modifizierten USB-Geräten“ an den Computer angeschlossen wurden, werden nach der Installation der Komponente als autorisiert betrachtet.

Um den Schutz vor modifizierten USB-Geräten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor modifizierten USB-Geräten** aus.
3. Verwenden Sie den Schalter **Schutz vor modifizierten USB-Geräten**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn Schutz vor modifizierten USB-Geräten aktiviert ist, erfordert Kaspersky Endpoint Security daher die Autorisierung eines angeschlossenen USB-Geräts, das vom Betriebssystem als Tastatur identifiziert wird. Der Benutzer kann eine nicht autorisierte Tastatur erst verwenden, nachdem sie autorisiert wurde.

Verwenden der Bildschirmtastatur für die Autorisierung von USB-Geräten

Die Möglichkeit zur Verwendung der Bildschirmtastatur ist nur für die Autorisierung von USB-Geräten vorgesehen, welche die Eingabe beliebiger Zeichen nicht unterstützen (z. B. Strichcode-Scanner). Es wird davon abgeraten, die Bildschirmtastatur für die Autorisierung unbekannter USB-Geräte zu verwenden.

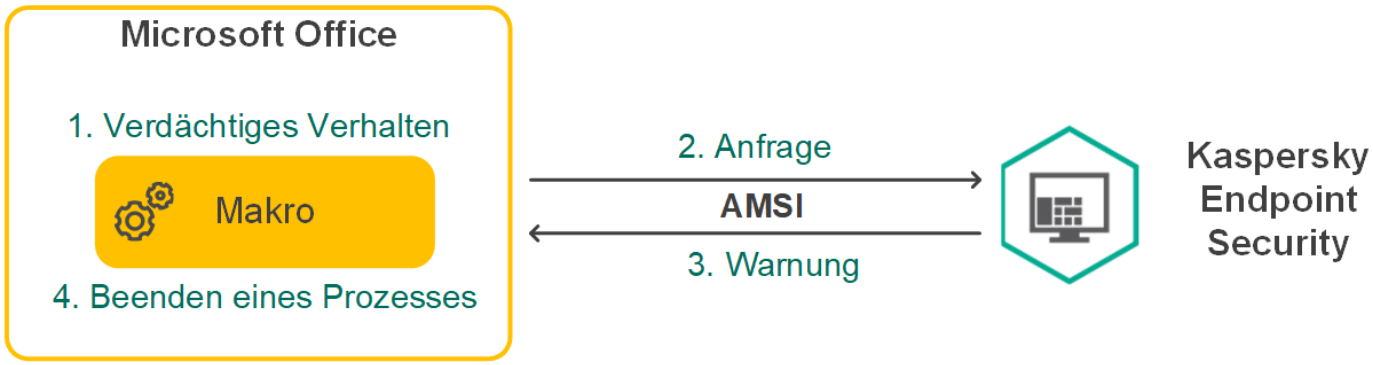
Um die Verwendung der Bildschirmtastatur bei der Autorisierung zu erlauben oder zu verbieten, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Schutz → Basisschutz → Schutz vor modifizierten USB-Geräten** aus.
3. Verwenden Sie das Kontrollkästchen **Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten**, um die Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten zu verbieten oder zuzulassen.
4. Speichern Sie die vorgenommenen Änderungen.

AMSI-Schutz

Die AMSI-Schutz-Komponente ist für die Unterstützung der Microsoft-Schnittstelle für „Antimalware Scan Interface“ vorgesehen. Mithilfe *Schnittstelle für Antimalware Scan Interface (AMSI)* können Drittthersteller-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Endpoint Security senden und Untersuchungsergebnisse für diese Objekte erhalten. Drittthersteller-Anwendungen können z. B. Microsoft-Office-Programme sein (siehe folgende Abb.). Details über die AMSI-Schnittstelle finden Sie in der *Dokumentation von Microsoft*.

Die Funktion von „AMSI-Schutz“ ist darauf beschränkt, eine Bedrohung zu erkennen und eine Drittanbieterprogramm über die gefundene Bedrohung zu benachrichtigen. Nachdem eine Drittthersteller-Anwendung über eine Bedrohung benachrichtigt wurde, verbietet sie die Ausführung schädlicher Aktionen (z. B. Programm beenden).



Beispiel für die Funktionsweise von AMSI

Die Komponente „AMSI-Schutz“ kann die Anfrage eines Drittanbieterprogramms zurückweisen. Dies ist beispielsweise möglich, wenn dieses Programm die maximale Anzahl von Anfragen innerhalb des festgelegten Zeitraums erreicht hat. Kaspersky Endpoint Security sendet Informationen über die Ablehnung der Anfrage einer Dritthersteller-Anwendung an den Administrationsserver. Die Komponente „AMSI-Schutz“ weist Anfragen von jenen Drittanbieterprogrammen nicht zurück, für die das Kontrollkästchen **Interaktion mit AMSI-Provider nicht blockieren** aktiviert ist.

“AMSI-Schutz“ ist für die folgenden Betriebssysteme für Workstations und Server verfügbar:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter.

“AMSI-Schutz“ aktivieren und deaktivieren

“AMSI-Schutz“ ist standardmäßig aktiviert.

Um „AMSI-Schutz“ zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Basisschutz** → **AMSI-Schutz** aus.
3. Verwenden Sie den Schalter **AMSI-Schutz**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Verwendung des AMSI-Schutzes zur Untersuchung zusammengesetzter Dateien

Eine häufige Methode, mit der Viren und andere bedrohliche Programme versteckt werden, ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Auswahl der Typen von zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

So konfigurieren Sie AMSI-Schutz-Untersuchungen von zusammengesetzten Dateien:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Basisschutz → AMSI-Schutz** aus.
3. Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.
4. Führen Sie unter **Größenbeschränkung** eine der folgenden Aktionen aus:
   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße** einen entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Schutz“ nicht entpackt.
   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Die Komponente „AMSI-Schutz“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.
5. Speichern Sie die vorgenommenen Änderungen.

Exploit-Prävention

Die Komponente „Exploit-Prävention“ überwacht Programmcode, der mithilfe eines Exploits Schwachstellen eines Computers ausnutzt, um dadurch Administratorrechte zu erhalten oder schädliche Aktionen auszuführen. Exploits können beispielsweise einen Angriff mit Überlauf der Zwischenablage verwenden. Dazu sendet der Exploit große Datenvolumen an ein verwundbares Programm. Bei der Verarbeitung dieser Daten führt das verwundbare Programm schädlichen Code aus. Aufgrund dieses Angriffs kann der Exploit eine nicht autorisierte Installation von Schadsoftware starten.

Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer ausgeführt wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei oder informiert den Benutzer.

Exploit-Prävention aktivieren und deaktivieren

Die Exploit-Prävention ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Bei Bedarf können Sie die Exploit-Prävention deaktivieren.

Um die Exploit-Prävention zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster den Abschnitt **Schutz → Erweiterter Schutz → Exploit-Prävention** aus.
3. Verwenden Sie den Schalter **Exploit-Prävention**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn Exploit-Prävention aktiviert ist, überwacht Kaspersky Endpoint Security ausführbare Dateien, die von verwundbaren Programmen ausgeführt werden. Wenn Kaspersky Endpoint Security erkennt, dass eine ausführbare Datei aus einem verwundbaren Programm nicht vom Benutzer gestartet wurde, führt Kaspersky Endpoint Security die ausgewählte Aktion aus (beispielsweise wird der Vorgang blockiert).

Aktion für den Fund eines Exploits auswählen

Beim Fund eines Exploits blockiert Kaspersky Endpoint Security standardmäßig die Aktivitäten dieses Exploits.

Um eine Aktion für den Fund eines Exploits auszuwählen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster den Abschnitt **Schutz → Erweiterter Schutz → Exploit-Prävention** aus.
3. Wählen Sie die entsprechende Aktion im Block **Wenn ein Exploit erkannt wird**:
   - **Vorgang blockieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.
   - **Informieren** Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über diesen Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.
4. Speichern Sie die vorgenommenen Änderungen.

Schutz für den Arbeitsspeicher von Systemprozessen

Der Schutz für den Arbeitsspeicher von Systemprozessen ist standardmäßig aktiviert.

Um den Schutz für den Arbeitsspeicher von Systemprozessen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster den Abschnitt **Schutz → Erweiterter Schutz → Exploit-Prävention** aus.
3. Verwenden Sie den Schalter **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**, um diese Funktion zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen blockiert Kaspersky Endpoint Security externe Prozesse, die versuchen, auf Systemprozesse zuzugreifen.

Verhaltensanalyse

Die Komponente „Verhaltensanalyse“ empfängt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt andere Schutzkomponenten mit diesen Informationen, um deren Effektivität zu erhöhen.

Die Komponente „Verhaltensanalyse“ verwendet Vorlagen für gefährliches Programmverhalten. Stimmt die Aktivität eines Programms mit einer der Aktivitäten aus den Vorlagen für gefährliches Verhalten überein, so führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Endpoint Security, die auf Vorlagen für gefährliches Verhalten beruht, bietet einen proaktiven Computerschutz.

Verhaltensanalyse aktivieren und deaktivieren

Die Verhaltensanalyse ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Bei Bedarf können Sie die Verhaltensanalyse deaktivieren.

Es wird davor gewarnt, die Verhaltensanalyse ohne triftigen Grund zu deaktivieren, da dies die Effektivität der Schutzkomponenten beeinträchtigt. Die Schutzkomponenten können die von der Verhaltensanalyse empfangenen Daten abfragen, um Bedrohungen zu erkennen.

Um die Verhaltensanalyse zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Verhaltensanalyse** aus.
3. Verwenden Sie den Schalter **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verhaltensanalyse aktiviert ist, verwendet Kaspersky Endpoint Security daher Vorlagen für gefährliches Verhalten, um die Aktivität von Programmen im Betriebssystem zu analysieren.

Aktion beim Fund schädlicher Programmaktivität wählen

Um eine Aktion für den Fund schädlicher Programmaktivität zu wählen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Verhaltensanalyse** aus.
3. Wählen Sie die entsprechende Aktion im Block **Wenn Schadsoftware-Aktivität erkannt wird**:

- **Datei löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.

- **Programm beenden**. Wenn dieses Element gewählt wird, beendet Kaspersky Endpoint Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.

- **Informieren** Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Endpoint Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.

4. Speichern Sie die vorgenommenen Änderungen.

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern

Die Komponente gewährleistet die Vorgangsnachverfolgung nur für jene Dateien, die sich auf Massenspeichergeräten mit NTFS-Dateisystem befinden und die nicht mit einem EFS-System verschlüsselt wurden.

Die Funktion zum Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern gewährleistet die Analyse von Aktivitäten in gemeinsamen Ordnern. Falls die Aktivität mit einer Vorlage für gefährliches Verhalten übereinstimmt, das für eine externe Verschlüsselung charakteristisch ist, so führt Kaspersky Endpoint Security die ausgewählte Aktion aus.

Der Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist standardmäßig deaktiviert.

Die Funktion für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist nach der Installation von Kaspersky Endpoint Security bis zum Neustart des Computers beschränkt.

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren und deaktivieren

Die Funktion für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist nach der Installation von Kaspersky Endpoint Security bis zum Neustart des Computers beschränkt.

Um den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Erweiterter Schutz → Verhaltensanalyse** aus.

3. Verwenden Sie den Schalter **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren**, um die Erkennung von Aktivitäten zu aktivieren oder zu deaktivieren, die für externe Verschlüsselung typisch sind.

4. Speichern Sie die vorgenommenen Änderungen.

Aktion auswählen, die beim Erkennen der externen Verschlüsselung gemeinsamer Ordner ausgeführt werden soll

Um die Aktion auszuwählen, die beim Erkennen der externen Verschlüsselung gemeinsamer Ordner ausgeführt werden soll, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Verhaltensanalyse** aus.
3. Wählen Sie die entsprechende Aktion im Abschnitt **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern**:
   - **Verbindung blockieren für n Min.** Ist diese Variante ausgewählt und es wird ein Versuch erkannt, Dateien in gemeinsamen Ordnern zu ändern, führt Kaspersky Endpoint Security die folgenden Aktionen aus:
     - Sperrung der Netzwerkaktivität des Computers, der die Änderung ausführt.
     - Erstellung von Backup-Kopien der Dateien, die geändert wurden.
     - Hinzufügen eines Eintrags zu den Berichten der lokalen Programmoberfläche.
     - Senden von Informationen über den Fund einer schädlichen Aktivität an Kaspersky Security Center.

     Ist dabei die Komponente „Rollback von schädlichen Aktionen“ aktiviert, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.
   - **Informieren** Ist diese Variante ausgewählt und es wird ein Versuch erkannt, Dateien in gemeinsamen Ordnern zu ändern, so führt Kaspersky Endpoint Security die folgenden Aktionen aus:
     - Hinzufügen eines Eintrags zu den Berichten der lokalen Programmoberfläche.
     - Fügt einen Eintrag zur Liste der aktiven Bedrohungen hinzu.
     - Senden von Informationen über den Fund einer schädlichen Aktivität an Kaspersky Security Center.
4. Speichern Sie die vorgenommenen Änderungen.

Eine Ausnahme für den Schutz von gemeinsamen Ordnern vor externer Verschlüsselung erstellen

Durch das Ausschließen eines Ordners lässt sich die Anzahl der Fehlalarme reduzieren, wenn Ihr Unternehmen bei der Dateiübertragung über gemeinsame Ordner eine Datenverschlüsselung verwendet. Beispielsweise kann die „Verhaltensanalyse“ Fehlalarme auslösen, wenn der Benutzer in einem gemeinsamen Ordner Dateien mit der Erweiterung ENC verwendet. Diese Aktivität gleicht einem Verhaltensmuster, das für externe Verschlüsselung charakteristisch ist. Wenn Sie zu Datenschutzzwecken verschlüsselte Dateien in einem gemeinsamen Ordner ablegen, fügen Sie diesen Ordner den Ausnahmen hinzu.

[So erstellen Sie über die Verwaltungskonsole (MMC) eine Ausnahme für den Schutz von gemeinsamen Ordnern]

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen** aus.
6. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf **Einstellungen**.
7. Wählen Sie im folgenden Fenster die Registerkarte **Untersuchungsausnahmen** aus.

   Dies öffnet ein Fenster mit einer Liste der Ausnahmen.
8. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.
9. Markieren Sie das Kontrollkästchen **Verwendung lokal vertrauenswürdiger Programme erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten Dateien weiterhin von Untersuchungen aus.
10. Klicken Sie auf **Hinzufügen**.
11. Aktivieren Sie unter **Eigenschaften** das Kontrollkästchen **Datei oder Ordner**.
12. Klicken Sie auf den Link **Datei oder Ordner wählen** im Abschnitt **Beschreibung der Untersuchungsausnahme (zum Ändern auf unterstrichene Elemente klicken)**, um das Fenster **Datei- oder Ordnername** zu öffnen.
13. Klicken Sie auf **Durchsuchen** und wählen Sie den gemeinsamen Ordner aus.

    Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

    - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.
    - Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske

`C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich in Ordnern innerhalb des Ordners `Folder` befinden, unter Ausnahme des Ordners `Folder` selbst. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.

- Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

14. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

15. Klicken Sie auf den Link **alle** im Abschnitt **Beschreibung der Untersuchungsausnahme (zum Ändern auf unterstrichene Elemente klicken)**, um den Link **Komponenten wählen** zu aktivieren.

16. Öffnen Sie mit dem Link **Komponenten wählen** das Fenster **Schutzkomponenten**.

17. Aktivieren Sie das Kontrollkästchen neben der Komponente **Verhaltensanalyse**.

18. Speichern Sie die vorgenommenen Änderungen.

[So erstellen Sie über die „Web Console“ oder „Cloud Console“ eine Ausnahme für den Schutz von gemeinsamen Ordnern]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Allgemeine Einstellungen** → **Ausnahmen** aus.
5. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf den Link **Untersuchungsausnahmen**.
6. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.
7. Markieren Sie das Kontrollkästchen **Verwendung lokal vertrauenswürdiger Programme erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten Dateien weiterhin von Untersuchungen aus.
8. Klicken Sie auf **Hinzufügen**.
9. Wählen Sie aus, welche Art von Ausnahme Sie hinzufügen möchten: **Datei oder Ordner**.
10. Klicken Sie auf **Durchsuchen** und wählen Sie den gemeinsamen Ordner aus.

    Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

    - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.
    - Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich in Ordnern innerhalb des Ordners `Folder` befinden, unter Ausnahme des Ordners `Folder` selbst. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.
    - Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

11. Wählen Sie im Block **Schutzkomponenten** die Komponente **Verhaltensanalyse** aus.
12. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.
13. Wählen Sie den Status **Aktiv** für die Ausnahme.

    Über den Schalter können Sie eine Ausnahme jederzeit stoppen.
14. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie über die Programmoberfläche eine Ausnahme für den Schutz von gemeinsamen Ordnern

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Punkt **Allgemeine Einstellungen** → **Gefahren und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie den gemeinsamen Ordner aus.

   Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

   - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.
   - Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung TXT, die sich in Ordnern innerhalb des Ordners `Folder` befinden, unter Ausnahme des Ordners `Folder` selbst. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.
   - Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.
6. Wählen Sie im Block **Schutzkomponenten** die Komponente **Verhaltensanalyse** aus.
7. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.
8. Wählen Sie den Status **Aktiv** für die Ausnahme.

   Über den Schalter können Sie eine Ausnahme jederzeit stoppen.
9. Speichern Sie die vorgenommenen Änderungen.

Adressen von Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern anpassen

Damit die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert, muss der Dienst für die Anmeldungsüberwachung aktiviert werden. Der Dienst für die Anmeldungsüberwachung ist standardmäßig deaktiviert (weitere Informationen über die Aktivierung der Anmeldungsüberwachung finden Sie auf der Website der Microsoft Corporation).

Die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert nicht, wenn der betreffende Remote-Computer bereits vor dem Start von Kaspersky Endpoint Security eingeschaltet war. Sie können diesen Remote-Computer nach dem Start von Kaspersky Endpoint Security neu starten, damit die Funktionalität, mit der Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, auf diesem Remote-Computer funktioniert.

Um bestimmte Remote-Computer, welche die externe Verschlüsselung von gemeinsamen Ordnern ausführen, vom Schutz auszuschließen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Erweiterter Schutz → Verhaltensanalyse** aus.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Adressen für Ausnahmen anpassen**.
4. Um die IP-Adresse oder den Namen eines Computers zur Ausnahmeliste hinzuzufügen, klicken Sie auf **Hinzufügen**.
5. Geben Sie die IP-Adresse oder den Namen des Computers ein, dessen Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.
6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste der Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern

Sie können die Liste der Ausnahmen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um die Listen der Erweiterungen zu sichern oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Fenster der Richtlinien **Erweiterter Schutz** → **Verhaltensanalyse** aus.
6. Klicken Sie im Block **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern** auf **Ausnahmen**.
7. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
8. So importieren Sie die Ausnahmeliste:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
9. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste der Erweiterungen in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste von Erweiterungen exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Verhaltensanalyse** aus.
5. So exportieren Sie die Liste der Ausnahmen im Block **Ausnahmen**:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.
   d. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   e. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
6. So importieren Sie die Liste der Ausnahmen im Block **Ausnahmen**:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

Programm-Überwachung

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Programm-Überwachung“ (HIPS, Host Intrusion Prevention System) hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken und des Cloud-Dienstes Kaspersky Security Network

Die Komponente kontrolliert Programme mithilfe von *Programmrechten*. Programmrechte beinhalten die folgenden Zugriffseinstellungen:

- Zugriff auf Betriebssystemressourcen (z. B. Autostart-Einstellungen und Registrierungsschlüssel)
- Zugriff auf persönliche Daten (z. B. auf Dateien und Programme)

Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.

Wenn ein Programm zum ersten Mal gestartet wird, führt die Komponente „Programm-Überwachung“ die folgenden Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.
2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Programm-Überwachung“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Das Programm wird einer *Sicherheitsgruppe* zugewiesen: Vertrauenswürdig, Schwach beschränkt, Stark beschränkt, Nicht vertrauenswürdig.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Aktionen des Programms. Für Programme aus der Sicherheitsgruppe „Stark beschränkt“ ist beispielsweise der Zugriff auf Module des Betriebssystems verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde ein Programm nicht verändert, so wendet die Komponente die aktuellen Rechte für Programme darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Programm-Überwachung aktivieren und deaktivieren

Die Programm-Überwachung ist standardmäßig aktiviert und läuft im Modus, der von Kaspersky empfohlen wird.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.
6. Verwenden Sie das Kontrollkästchen **Programm-Überwachung**, um die Komponente zu aktivieren oder zu deaktivieren.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Verwenden Sie den Schalter **Programm-Überwachung**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Verwenden Sie den Schalter **Programm-Überwachung**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Komponente „Programm-Überwachung“ aktiviert ist, fügt Kaspersky Endpoint Security Programme zu Sicherheitsgruppen hinzu und berücksichtigt dabei die Stufe der Bedrohung, die das jeweilige Programm für den Computer darstellen kann. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe.

Sicherheitsgruppe für Programme verwenden

Wenn ein Programm zum ersten Mal gestartet wird, überprüft die Komponente „Programm-Überwachung“, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu.

Beim ersten Schritt überprüft Kaspersky Endpoint Security, ob das Programm in der internen Datenbank für bekannte Programme verzeichnet ist, und sendet gleichzeitig eine Anfrage an die Datenbank von Kaspersky Security Network (sofern eine Internetverbindung besteht). Abhängig von den Ergebnissen der Überprüfung mit der internen Datenbank und der Datenbank von Kaspersky Security Network wird das Programm einer Sicherheitsgruppe zugeordnet. Bei jedem künftigen Programmstart sendet Kaspersky Endpoint Security eine neue Anfrage an die KSN-Datenbank, und weist das Programm einer anderen Sicherheitsgruppe zu, falls sich die Reputation des Programms in der KSN-Datenbank geändert hat.

Sie können eine Sicherheitsgruppe auswählen, in die Kaspersky Endpoint Security alle unbekannten Programme automatisch verschieben soll. Programme, die vor Kaspersky Endpoint Security gestartet wurden, werden automatisch der Sicherheitsgruppe zugeordnet, die im Fenster mit den Einstellungen der Komponente „Programm-Überwachung“ festgelegt ist.

Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt gemäß den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind.

Die Sicherheitsgruppe eines Programms ändern

Wenn ein Programm zum ersten Mal gestartet wird, überprüft die Komponente „Programm-Überwachung“, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu.

Die Kaspersky-Experten warnen davor, Programme aus einer Sicherheitsgruppe, der sie automatisch zugewiesen wurde, in andere Sicherheitsgruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Rechte für ein bestimmtes Programm.

So ändern Sie die Sicherheitsgruppe eines Programms in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.
6. Klicken Sie im Block **Programmrechte** auf die Schaltfläche **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
7. Wählen Sie die Registerkarte **Rechte für Programme** aus.
8. Klicken Sie auf **Hinzufügen**.
9. Geben Sie im nächsten Fenster Kriterien ein, um nach dem Programm zu suchen, dessen Sicherheitsgruppe Sie ändern möchten.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
10. Klicken Sie auf **Aktualisieren**.

    Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.
11. Wählen Sie das erforderliche Programm.
12. Wählen Sie in der Dropdown-Liste **Ausgewählte Programme zu <Sicherheitsgruppe> hinzufügen** die gewünschte Sicherheitsgruppe für das Programm aus.
13. Speichern Sie die vorgenommenen Änderungen.

[So ändern Sie die Sicherheitsgruppe des Programms in der Web Console und der Cloud Console](#)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Wählen Sie die Registerkarte **Rechte für Programme** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.
8. Klicken Sie auf den Link **Ausgewählte Zielgruppe**, um die gewünschte Sicherheitsgruppe für das Programm auszuwählen.
9. Wählen Sie den **Programm**typ aus. Klicken Sie auf **Weiter**.

   Wenn Sie die Sicherheitsgruppe für mehrere Programme ändern möchten, wählen Sie den Typ der **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.
10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, deren Sicherheitsgruppe Sie ändern möchten.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
11. Schließen Sie den Assistenten mit einem Klick auf **OK** ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.
12. Speichern Sie die vorgenommenen Änderungen.

[So ändern Sie die Sicherheitsgruppe eines Programms in der Programmoberfläche]

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Klicken Sie auf die Schaltfläche **Programme verwalten**.

   Dadurch wird die Liste der installierten Programme geöffnet.
4. Wählen Sie das erforderliche Programm.
5. Wählen Sie im Kontextmenü des Programms den Punkt **Einschränkungen** → <Σιχηερηειτσγρυππε> aus.
6. Speichern Sie die vorgenommenen Änderungen.

Daraufhin wird das Programm zu einer anderen Sicherheitsgruppe hinzugefügt. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe. Dem Programm wird der Status *(benutzerdefiniert)* zugewiesen. Wenn sich die Reputation des Programms in Kaspersky Security Network ändert, lässt die Komponente „Programm-Überwachung“ die Sicherheitsgruppe dieses Programms unverändert.

Rechte von Sicherheitsgruppen konfigurieren

Die optimalen Programmrechte werden standardmäßig für verschiedene Sicherheitsgruppen erstellt. Die Einstellungen für die Rechte von Programmgruppen, die zu einer Sicherheitsgruppe gehören, erben die Einstellungswerte der Rechte für die Sicherheitsgruppen.

So ändern Sie die Rechte von Sicherheitsgruppen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Klicken Sie im Block **Programmrechte** auf die Schaltfläche **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
7. Wählen Sie die Registerkarte **Rechte für Programme** aus.
8. Wählen Sie die gewünschte Sicherheitsgruppe aus.
9. Wählen Sie **Gruppenrechte** aus dem Kontextmenü der Sicherheitsgruppe.

   Die Eigenschaften der Sicherheitsgruppe werden geöffnet.
10. Führen Sie eine der folgenden Aktionen aus:

    - Wählen Sie die Registerkarte **Dateien und Systemregistrierung** aus, um die Sicherheitsgruppenrechte zu ändern, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln.
    - Wählen Sie die Registerkarte **Rechte** aus, um die Sicherheitsgruppenrechte zu ändern, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln.

    Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.
11. Öffnen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion mit einem Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (⊘).
12. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** (✓ / ⊘).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.
13. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Rechte einer Sicherheitsgruppe in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Wählen Sie die Registerkarte **Rechte für Programme** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Wählen Sie im linken Bereich des Fensters die gewünschte Sicherheitsgruppe aus.
8. Führen Sie im rechten Bereich des Fensters in der Dropdown-Liste eine der folgenden Aktionen aus:

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

   Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.
9. Wählen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (✗).
10. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** (✓ / ✗).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.
11. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie Sicherheitsgruppenrechte in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Klicken Sie auf die Schaltfläche **Programme verwalten**.

   Dadurch wird die Liste der installierten Programme geöffnet.
4. Wählen Sie die gewünschte Sicherheitsgruppe aus.
5. Wählen Sie im Kontextmenü der Sicherheitsgruppe den Punkt **Details und Regeln** aus.

   Die Eigenschaften der Sicherheitsgruppe werden geöffnet.
6. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie die Registerkarte **Dateien und Systemregistrierung** aus, um die Sicherheitsgruppenrechte zu ändern, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln.
   - Wählen Sie die Registerkarte **Rechte** aus, um die Sicherheitsgruppenrechte zu ändern, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln.

   Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.
7. Öffnen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion mit einem Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** () oder **Verbieten** ().
8. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** ().

   Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.
9. Speichern Sie die vorgenommenen Änderungen.

Die Rechte der Sicherheitsgruppe werden geändert. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe. Der Status (*Benutzereinstellungen*) wird der Sicherheitsgruppe zugewiesen.

Sicherheitsgruppe für Programme wählen, die vor Kaspersky Endpoint Security gestartet werden

Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt gemäß den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind. Um festzulegen, durch welche Netzwerkregeln die Kontrolle der Netzwerkaktivität solcher Programme reguliert werden soll, muss eine Sicherheitsgruppe angegeben werden.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Klicken Sie im Block **Programmrechte** auf die Schaltfläche **Bearbeiten**.
7. Wählen Sie die gewünschte Sicherheitsgruppe für die Einstellung **Programme, die vor Kaspersky Endpoint Security für Windows gestartet werden, automatisch in die Sicherheitsgruppe <Sicherheitsgruppe> verschieben**.
8. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz → Programm-Überwachung** aus.
5. Wählen Sie die gewünschte Sicherheitsgruppe für die Einstellung **Programme, die vor Kaspersky Endpoint Security für Windows gestartet werden, automatisch in die Sicherheitsgruppe <Sicherheitsgruppe> verschieben**.
6. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Erweiterter Schutz → Programm-Überwachung** aus.
3. Wählen Sie die gewünschte Sicherheitsgruppe im Block **Programme, die vor Kaspersky Endpoint Security für Windows gestartet werden, automatisch in die Sicherheitsgruppe <Sicherheitsgruppe> verschieben**.
4. Speichern Sie die vorgenommenen Änderungen.

Von nun an werden Programme, die vor Kaspersky Endpoint Security gestartet werden, zu einer anderen Sicherheitsgruppe hinzugefügt. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe.

Eine Sicherheitsgruppe für unbekannte Programme auswählen

Wenn ein Programm zum ersten Mal gestartet wird, ermittelt die Komponente „Programm-Überwachung“ die geeignete Sicherheitsgruppe für das Programm. Wenn Sie keinen Internetzugang haben oder wenn Kaspersky Security Network keine Informationen zu diesem Programm hat, ordnet Kaspersky Endpoint Security das Programm standardmäßig der Gruppe „Schwach beschränkt“ zu. Sobald Informationen zu einem zuvor unbekannten Programm in KSN gefunden werden, aktualisiert Kaspersky Endpoint Security die Rechte dieses Programms. Die Programmrechte können danach manuell angepasst werden.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Verwenden Sie im Block **Regeln zur Verarbeitung von Programmen** die Dropdown-Liste **Sicherheitsgruppe für Programme, die keiner anderen Gruppe zugewiesen werden konnten**, um die gewünschte Sicherheitsgruppe auszuwählen.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.
7. Verwenden Sie das Kontrollkästchen **Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.
8. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Verwenden Sie im Block **Regeln zur Verarbeitung von Programmen** die Dropdown-Liste **Sicherheitsgruppe für Programme, die keiner anderen Gruppe zugewiesen werden konnten**, um die gewünschte Sicherheitsgruppe auszuwählen.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.
6. Verwenden Sie das Kontrollkästchen **Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.
7. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Wählen Sie im Block **Vertrauensgruppe für unbekannte Programme** die entsprechende Vertrauensgruppe aus.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.
4. Verwenden Sie das Kontrollkästchen **Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.
5. Speichern Sie die vorgenommenen Änderungen.

Eine Sicherheitsgruppe für digital signierte Programme wählen

Programme, die mit Microsoft-Zertifikaten oder mit Kaspersky-Zertifikaten signiert sind, werden von Kaspersky Endpoint Security immer der Sicherheitsgruppe „Vertrauenswürdig“ zugeordnet.

So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme, die eine digitale Signatur eines vertrauenswürdigen Herstellers haben, die automatische Zuweisung zur Sicherheitsgruppe „Vertrauenswürdig“ zu aktivieren und deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.
7. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz → Programm-Überwachung** aus.
5. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme, die eine digitale Signatur eines vertrauenswürdigen Herstellers haben, die automatische Zuweisung zur Sicherheitsgruppe „Vertrauenswürdig“ zu aktivieren und deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.
6. Speichern Sie die vorgenommenen Änderungen.

[So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Programmoberfläche]

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme, die eine digitale Signatur eines vertrauenswürdigen Herstellers haben, die automatische Zuweisung zur Sicherheitsgruppe „Vertrauenswürdig“ zu aktivieren und deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.
4. Speichern Sie die vorgenommenen Änderungen.

Verwendung von Rechten für Programme

Standardmäßig basiert die Aktivitätskontrolle für Programme auf Programmrechten. Diese Rechte werden für die jeweilige Sicherheitsgruppe festgelegt, in die das Programm bei seinem ersten Start von Kaspersky Endpoint Security verschoben wurde. Bei Bedarf können Sie die Programmrechte für eine gesamte Sicherheitsgruppe, für ein einzelnes Programm oder für eine Programmgruppe innerhalb einer Sicherheitsgruppe bearbeiten.

Manuell festgelegte Programmrechte haben eine höhere Priorität als Programmrechte, die für eine Sicherheitsgruppe festgelegt wurden. Mit anderen Worten: Wenn manuell angelegte Programmrechte sich von den für die Sicherheitsgruppe festgelegten Programmrechten unterscheiden, kontrolliert die Komponente „Programm-Überwachung“ die Programmaktivität gemäß den manuell angelegten Programmrechten.

Die Regeln, die Sie für Programme erstellen, werden für untergeordnete Programme übernommen. Wenn Sie beispielsweise alle Netzwerkaktivitäten für cmd.exe verbieten, so werden auch für notepad.exe alle Netzwerkaktivitäten verboten, wenn dieses Programm über cmd.exe gestartet wird. Wenn ein Programm indirekt von einem anderen Programm gestartet wird, jedoch nicht dem Programm untergeordnet ist, von dem es ausgeführt wird, so werden die Regeln nicht vererbt.

[So ändern Sie die Programmrechte in der Verwaltungskonsole (MMC)]

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Klicken Sie im Block **Programmrechte** auf die Schaltfläche **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
7. Wählen Sie die Registerkarte **Rechte für Programme** aus.
8. Klicken Sie auf **Hinzufügen**.
9. Geben Sie im nächsten Fenster Kriterien ein, um nach dem Programm zu suchen, dessen Programmrechte Sie ändern möchten.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
10. Klicken Sie auf **Aktualisieren**.

    Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.
11. Wählen Sie das erforderliche Programm.
12. Wählen Sie in der Dropdown-Liste **Ausgewählte Programme zu <Sicherheitsgruppe> hinzufügen** den Punkt **Standardgruppen** aus und klicken Sie auf **OK**.

    Das Programm wird der Standardgruppe hinzugefügt.
13. Wählen Sie das gewünschte Programm aus und klicken Sie dann auf **Rechte für Programme** im Kontextmenü des Programms.

    Dadurch werden die Programmeigenschaften geöffnet.
14. Führen Sie eine der folgenden Aktionen aus:

    - Wählen Sie die Registerkarte **Dateien und Systemregistrierung** aus, um die Sicherheitsgruppenrechte zu ändern, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln.
    - Wählen Sie die Registerkarte **Rechte** aus, um die Sicherheitsgruppenrechte zu ändern, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln.

    Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.
15. Öffnen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion mit einem Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (⊘).

16. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** (/).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

17. Speichern Sie die vorgenommenen Änderungen.

[So ändern Sie die Programmrechte in der Web Console und der Cloud Console](#)

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Wählen Sie die Registerkarte **Rechte für Programme** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.
8. Klicken Sie auf den Link **Ausgewählte Zielgruppe**, um die gewünschte Sicherheitsgruppe für das Programm auszuwählen.
9. Wählen Sie den **Programm**typ aus. Klicken Sie auf **Weiter**.

   Wenn Sie die Sicherheitsgruppe für mehrere Programme ändern möchten, wählen Sie den Typ der **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.
10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, deren Programmrechte Sie ändern möchten.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
11. Schließen Sie den Assistenten mit einem Klick auf **OK** ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.
12. Klicken Sie im linken Fensterbereich auf das gewünschte Programm.
13. Führen Sie im rechten Bereich des Fensters in der Dropdown-Liste eine der folgenden Aktionen aus:

    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

    Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.
14. Wählen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (✗).

15. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** (/).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

16. Speichern Sie die vorgenommenen Änderungen.

[So ändern Sie Programmrechte in der Programmoberfläche](#)

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Klicken Sie auf die Schaltfläche **Programme verwalten**.

   Dadurch wird die Liste der installierten Programme geöffnet.
4. Wählen Sie das erforderliche Programm.
5. Wählen Sie im Kontextmenü des Programms den Punkt **Details und Regeln** aus.

   Dadurch werden die Programmeigenschaften geöffnet.
6. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie die Registerkarte **Dateien und Systemregistrierung** aus, um die Sicherheitsgruppenrechte zu ändern, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln.
   - Wählen Sie die Registerkarte **Rechte** aus, um die Sicherheitsgruppenrechte zu ändern, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln.
7. Öffnen Sie bei der gewünschten Ressource in der Spalte der entsprechenden Aktion mit einem Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** () oder **Verbieten** ().
8. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **In Bericht schreiben** ().

   Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.
9. Wählen Sie die Registerkarte **Ausnahmen** und konfigurieren Sie die erweiterten Einstellungen des Programms (siehe Tabelle unten).
10. Speichern Sie die vorgenommenen Änderungen.

Erweiterte Einstellungen des Programms

Einstellung	Beschreibung
Zu öffnende Dateien nicht untersuchen	Alle Dateien, die vom Programm geöffnet werden, sind von der Überprüfung durch Kaspersky Endpoint Security ausgeschlossen. Wenn Sie z. B. Programme zur Sicherung von Dateien verwenden, trägt diese Funktion dazu bei, den Ressourcenverbrauch von Kaspersky Endpoint Security zu reduzieren.
Programmaktivität nicht kontrollieren	Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität des Programms im Betriebssystem nicht. Die Programmaktivität wird durch die folgenden Komponenten überwacht: Verhaltensanalyse, Exploit-Prävention, Programm-Überwachung, Rollback von schädlichen Aktionen und Firewall.
Beschränkungen des übergeordneten Prozesses	Die für den übergeordneten Prozess konfigurierten Einschränkungen werden von Kaspersky Endpoint Security nicht auf einen untergeordneten Prozess angewendet. Der übergeordnete Prozess wird von einem Programm gestartet, für das Programmrechte (Host Intrusion Prevention) und Netzwerkregeln für das Programm (Firewall) konfiguriert sind.

(Programms) nicht übernehmen	
Aktivität der Unterprogramme nicht kontrollieren	Kaspersky Endpoint Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden.
Interaktion mit der Schnittstelle von Kaspersky Endpoint Security ermöglichen	Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security blockiert alle Versuche, Programme von einem Remote-Computer aus zu verwalten. Ist dieses Kontrollkästchen aktiviert, wird einem Remote-Administrationsprogramm erlaubt, Einstellungen für Kaspersky Endpoint Security über die Benutzeroberfläche von Kaspersky Endpoint Security zu verwalten.
Verschlüsselten Datenverkehr nicht untersuchen / Gesamten Datenverkehr nicht untersuchen	Der von diesem Programm initiierte Netzwerkverkehr wird von den Untersuchungen durch Kaspersky Endpoint Security ausgeschlossen. Sie können entweder den gesamten Verkehr oder nur den verschlüsselten Verkehr von den Untersuchungen ausschließen. Sie können auch einzelne IP-Adressen und Portnummern von Untersuchungen ausschließen.

Schutz für Betriebssystemressourcen und persönliche Daten

Die Komponente „Programm-Überwachung“ verwaltet die Rechte von Programmen hinsichtlich ihren Vorgängen mit diversen Ressourcenkategorien des Betriebssystems und persönlichen Daten. Die Kaspersky-Experten haben Kategorien für geschützte Ressourcen vordefiniert. So enthält z. B. die Kategorie *Betriebssystem* die Unterkategorie *Starteinstellungen*, in der alle Registrierungsschlüssel aufgelistet sind, die mit dem Autostart von Programmen verknüpft sind. Die für geschützte Ressourcen vorgegebenen Kategorien und die damit zusammenhängenden geschützten Ressourcen können nicht geändert oder gelöscht werden.

Hinzufügen oder Löschen einer geschützten Ressource in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.
6. Klicken Sie im Block **Programmrechte** auf die Schaltfläche **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
7. Wählen Sie die Registerkarte **Geschützte Ressourcen** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit geschützten Ressourcen und die entsprechenden Rechte für den Zugriff auf diese Ressourcen, abhängig von der jeweiligen Sicherheitsgruppe.
8. Wählen Sie die Kategorie der geschützten Ressourcen aus, zu der Sie eine neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, klicken Sie auf **Hinzufügen** → **Kategorie**.
9. Klicken Sie auf **Hinzufügen**. Wählen Sie in der Dropdown-Liste den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.
10. Wählen Sie im geöffneten Fenster eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.

    Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin die Zugriffsrechte für jede Sicherheitsgruppe an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe des Kontrollkästchens neben der neuen Ressource deaktiviert werden.
11. Speichern Sie die vorgenommenen Änderungen.

[So fügen Sie eine geschützte Ressource in der Web Console und der Cloud Console hinzu]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Wählen Sie die Registerkarte **Geschützte Ressourcen** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit geschützten Ressourcen und die entsprechenden Rechte für den Zugriff auf diese Ressourcen, abhängig von der jeweiligen Sicherheitsgruppe.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Ressourcen wird gestartet.
8. Klicken Sie auf den Link **Gruppenname**, um die Kategorie der geschützten Ressourcen auszuwählen, zu der Sie die neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, wählen Sie die Option **Kategorie für geschützte Ressourcen** aus.
9. Wählen Sie den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.
10. Wählen Sie eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.
11. Schließen Sie den Assistenten mit einem Klick auf **OK** ab.

    Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin die Zugriffsrechte für jede Sicherheitsgruppe an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe des Kontrollkästchens in der Spalte **Status** deaktiviert werden.
12. Speichern Sie die vorgenommenen Änderungen.

[So fügen Sie eine geschützte Ressource in der Programmoberfläche hinzu](#)

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Klicken Sie auf die Schaltfläche **Ressourcen verwalten**.

   Die Liste der geschützten Ressourcen wird geöffnet.
4. Wählen Sie die Kategorie der geschützten Ressourcen aus, zu der Sie eine neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, klicken Sie auf **Hinzufügen** → **Kategorie**.
5. Klicken Sie auf **Hinzufügen**. Wählen Sie in der Dropdown-Liste den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.
6. Wählen Sie im geöffneten Fenster eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.

   Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin eine Liste mit Programmen und die Zugriffsrechte für jedes Programm an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe der Schaltfläche **Kontrolle deaktivieren** in der Spalte **Status** deaktiviert werden.
7. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Endpoint Security steuert den Zugriff auf die hinzugefügten Betriebssystemressourcen und auf persönliche Daten. Kaspersky Endpoint Security steuert den Zugriff eines Programms auf Ressourcen unter Berücksichtigung der Sicherheitsgruppe, die dem Programm zugewiesen wurde. Die Sicherheitsgruppe eines Programms kann geändert werden.

Löschen von Informationen über nicht verwendete Programme

Kaspersky Endpoint Security kontrolliert mithilfe von Programmrechten die Verwendung von Programmen. Die Rechte eines Programms sind von der Sicherheitsgruppe abhängig. Kaspersky Endpoint Security ordnet ein Programm einer Sicherheitsgruppe zu, wenn das Programm zum ersten Mal gestartet wird. Sie können die Sicherheitsgruppe für ein Programm manuell ändern. Außerdem können Sie die Rechte für ein bestimmtes Programm manuell anpassen. Kaspersky Endpoint Security speichert die folgenden Informationen über ein Programm: Sicherheitsgruppe und Rechte des Programms.

Kaspersky Endpoint Security löscht automatisch Informationen über nicht verwendete Programme, um Computer-Ressourcen zu sparen. Um Informationen über Programme zu löschen, richtet sich Kaspersky Endpoint Security nach folgenden Regeln:

- Wenn die Sicherheitsgruppe und die Programmrechte automatisch festgelegt wurden, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 30 Tagen. Es ist nicht möglich, die Speicherdauer für Informationen über ein Programm zu ändern oder das automatische Löschen zu deaktivieren.
- Wenn Sie das Programm einer Sicherheitsgruppe zugewiesen oder die Programmrechte manuell angepasst haben, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 60 Tagen (Standardwert). Sie können die Speicherdauer für Informationen über das Programm ändern oder das automatische Löschen deaktivieren (siehe Anleitung unten).

Wenn ein Programm gestartet wird, über das Informationen gelöscht wurden, untersucht Kaspersky Endpoint Security das Programm wie beim ersten Start.

[So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Verwaltungskonsole (MMC)]

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.
6. Führen Sie unter **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:
   - Um das automatische Löschen anzupassen, aktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen** und geben Sie die gewünschte Anzahl der Tage an.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.
   - Um das automatische Löschen auszuschalten, deaktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.
7. Speichern Sie die vorgenommenen Änderungen.

[So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Web Console und der Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Programm-Überwachung** aus.
5. Führen Sie unter **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:

   - Um das automatische Löschen anzupassen, aktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen** und geben Sie die gewünschte Anzahl der Tage an.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

   - Um das automatische Löschen auszuschalten, deaktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz → Erweiterter Schutz → Programm-Überwachung** aus.
3. Führen Sie unter **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:
   - Um das automatische Löschen anzupassen, aktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen** und geben Sie die gewünschte Anzahl der Tage an.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.
   - Um das automatische Löschen auszuschalten, deaktivieren Sie das Kontrollkästchen **Rechte für Programme löschen, wenn nicht gestartet seit n Tagen**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.
4. Speichern Sie die vorgenommenen Änderungen.

Übersicht über die Programm-Überwachung

Sie können Berichte über den Betrieb der Komponente „Programm-Überwachung“ abrufen. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

Um den Betrieb der „Programm-Überwachung“ zu verfolgen, müssen Sie das Erstellen von Berichten aktivieren. So können Sie z. B. die Weiterleitung von Berichten für einzelne Programme in den Einstellungen der Komponente „Programm-Überwachung“ aktivieren.

Berücksichtigen Sie bei der Konfiguration von „Programm-Überwachung“ die mögliche Netzwerkauslastung, wenn Sie Ereignisse an Kaspersky Security Center weiterleiten. Alternativ kann das Speichern von Berichten nur im lokalen Protokoll von Kaspersky Endpoint Security aktiviert werden.

Schutz des Zugriffs auf Audio und Video

Cyberkriminelle können mithilfe spezieller Programme versuchen, auf Geräte zuzugreifen, die Audio und Video aufzeichnen (z. B. Mikrofone und Webcams). Kaspersky Endpoint Security steuert, wann ein Programm einen Audio- oder Videostream empfangen darf, und schützt Daten vor unbefugtem Abfangen.

Standardmäßig steuert Kaspersky Endpoint Security den Zugriff von Programmen auf den Audio- und Videostream basierend auf der Programmkategorie:

- Programme der Kategorie „Vertrauenswürdig“ und „Schwach beschränkt“ dürfen standardmäßig den Audio- und Videostream von Geräten empfangen.
- Programme der Kategorie „Stark beschränkt“ und „Nicht vertrauenswürdig“ dürfen den Audio- und Videostream von Geräten standardmäßig nicht empfangen.

Es ist möglich, Programmen manuell zu erlauben, den Audio- und Videostream zu empfangen.

Besondere Funktionen zum Schutz des Audiostreams

Die Funktionalität zum Schutz des Audiostreams besitzt folgende Besonderheiten:

- Damit die Funktionalität einwandfrei funktioniert, muss die Komponente „Programm-Überwachung“ aktiviert sein.
- Hat ein Programm bereits begonnen, ein Audiosignal zu empfangen, bevor die Komponente „Programm-Überwachung“ gestartet wurde, so erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.
- Wenn Sie ein Programm in die Gruppe „Nicht vertrauenswürdig“ oder „Stark beschränkt“ verschoben haben, nachdem das Programm bereits begonnen hat, einen Audiostream zu empfangen, erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiostreams und zeigt keine Benachrichtigungen an.
- Nachdem die Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte geändert werden (wenn z. B. einem Programm verboten wird, den Audiostream zu empfangen), muss dieses Programm neu gestartet werden, damit es keinen Audiostream mehr empfängt.
- Die Kontrolle für den Empfang des Audiosignals von Tonaufnahmegeräten ist nicht von den Einstellungen für den Webcam-Schutz abhängig.
- Kaspersky Endpoint Security schützt nur den Zugriff auf integrierte und externe Mikrofone. Andere Tonübertragungsgeräte werden nicht unterstützt.
- Für Audiosignale, die von Geräten wie DSLR-Kameras, tragbaren Videokameras und Action-Cams übertragen werden, kann das Programm Kaspersky Endpoint Security keinen Schutz garantieren.
- Wenn Kaspersky Endpoint Security nach der Installation zum ersten Mal gestartet wird, kann es vorkommen, dass die Wiedergabe oder Aufzeichnung von Audio- und Videodaten in entsprechenden Programmen abgebrochen wird. Dies ist erforderlich, um die Überwachung des Zugriffs von Programmen auf Tonaufnahmegeräte zu aktivieren. Der Systemdienst für die Verwaltung von Audiogeräten wird beim ersten Start des Programms Kaspersky Endpoint Security neu gestartet.

Besondere Funktionen zum Schutz des Zugriffs von Programmen auf die Webcam

Die Funktionalität für den Webcam-Schutz besitzt folgende Besonderheiten und Einschränkungen:

- Das Programm kontrolliert Videos und statische Bilder, die auf Webcam-Daten basieren.
- Das Programm kontrolliert Audiosignale, wenn diese zu einem Videostream der Webcam gehören.
- Das Programm kontrolliert nur Webcams, die über eine USB-Schnittstelle oder IEEE1394-Schnittstelle angeschlossen und im Microsoft Geräte-Manager als **Gerät zur Bildverarbeitung** (Imaging Device) angezeigt

werden.

- Kaspersky Endpoint Security unterstützt folgende Webcams:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky garantiert nicht, dass Webcams, die nicht in dieser Liste genannt sind, unterstützt werden.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- **Dateiaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht ausführbare Dateien, die von Schadsoftware erstellt wurden (auf allen Datenträgern, außer auf Netzlaufwerken).
  - löscht ausführbare Dateien, die von Programmen erstellt wurden, in welche Schadsoftware eingedrungen ist.
  - stellt Dateien wieder her, die von Schadsoftware verändert oder gelöscht wurden.

  Die Funktionalität zur Wiederherstellung von Dateien besitzt bestimmte Beschränkungen.

- **Aktivität der Registrierung**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.
  - stellt Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden, nicht wieder her.

- **Systemaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - beendet Prozesse, die von Schadsoftware gestartet wurden.
  - beendet Prozesse, in die Schadsoftware eingedrungen ist.
  - stellt Prozesse, die von Schadsoftware beendet wurden, nicht wieder her.

- **Netzwerkaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - verbietet die Netzwerkaktivität von Schadsoftware.
  - verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback von Schadsoftware-Aktionen kann entweder von der Komponente Schutz vor bedrohlichen Dateien, Verhaltensanalyse oder bei einer Untersuchung auf Viren gestartet werden.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich eine eng eingeschränkte Auswahl an Daten. Ein Rollback hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und die Integrität der Daten auf Ihrem Computer.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Fenster der Richtlinien **Erweiterter Schutz** → **Rollback von schädlichen Aktionen** aus.
6. Verwenden Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, um die Komponente zu aktivieren oder zu deaktivieren.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Schutz** → **Rollback von schädlichen Aktionen** aus.
5. Verwenden Sie den Schalter **Rollback von schädlichen Aktionen**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Rollback von schädlichen Aktionen** aus.
3. Verwenden Sie den Schalter **Rollback von schädlichen Aktionen**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn Rollback von schädlichen Aktionen aktiviert ist, rollt Kaspersky Endpoint Security die von bösartigen Programmen im Betriebssystem ausgeführten Aktionen zurück.

Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. Wenn Sie an Kaspersky Security Network teilnehmen, erhält das Programm Kaspersky Endpoint Security von den KSN-Diensten Informationen über die Kategorie und die Reputation untersuchter Dateien, sowie Informationen über die Reputation untersuchter Webadressen.

Die Verwendung von Kaspersky Security Network ist freiwillig. Das Programm schlägt während der Erstkonfiguration des Programms vor, KSN zu verwenden. Die KSN-Nutzung kann jederzeit begonnen oder beendet werden.

Ausführliche Informationen darüber, welche Informationen an Kaspersky gesendet werden und wie statistische Informationen gespeichert und gelöscht werden, finden Sie in der „Erklärung zu Kaspersky Security Network“ und auf der Website von Kaspersky. Die Datei ksn_<Sprach-ID>.txt mit dem Text der Vereinbarung über Kaspersky Security Network ist im Lieferumfang des Programms enthalten.

Um die Auslastung der KSN-Server zu reduzieren, kann Kaspersky Programm-Updates veröffentlichen, welche die Zugriffsmöglichkeit auf das Kaspersky Security Network vorübergehend deaktivieren oder teilweise einschränken. In diesem Fall wird auf der lokalen Programmoberfläche der KSN-Verbindungsstatus *Aktiviert mit Einschränkungen* angezeigt.

KSN-Infrastruktur

Kaspersky Endpoint Security unterstützt die folgenden KSN-Infrastruktur-Lösungen:

- Die Lösung *Global KSN* wird von den meisten Kaspersky-Programmen verwendet. Die KSN-Teilnehmer erhalten von Kaspersky Security Network Informationen und senden an Kaspersky bestimmte Daten über Objekte, die auf dem Benutzercomputer gefunden wurden. Auf diese Weise können die Daten zusätzlich durch die Kaspersky-Analytiker untersucht werden, und die Reputations- und Statistik-Datenbanken von Kaspersky Security Network werden ergänzt.

- Die Lösung *Private KSN* ermöglicht Benutzern den Zugriff auf die Reputations-Datenbanken und auf andere statistische Daten, ohne dabei Daten von den Benutzercomputern an KSN zu senden. Auf diesen Computern müssen das Programm Kaspersky Endpoint Security oder andere Kaspersky-Programme installiert sein. Private KSN wurde für Unternehmenskunden entwickelt, die z. B. aus folgenden Gründen keine Möglichkeit zur Teilnahme an Kaspersky Security Network haben:

  - Lokale Arbeitsplätze haben keinen Internetzugriff.

  - Es ist gesetzlich verboten oder durch die Unternehmenssicherheit beschränkt, beliebige Daten in andere Länder oder aus dem lokalen Unternehmensnetzwerk heraus zu senden.

Kaspersky Security Center verwendet standardmäßig Global KSN. Die Verwendung von Private KSN können Sie in der Verwaltungskonsole (MMC), in der Kaspersky Security Center 12 Web Console und über die Befehlszeile anpassen. Es ist nicht möglich, die Verwendung von Private KSN in Kaspersky Security Center Cloud Console anzupassen.

Details über die Funktionsweise von Private KSN finden Sie in der *Dokumentation zu Kaspersky Private Security Network*.

KSN Proxy

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können zur Interaktion mit KSN den Dienst KSN Proxy verwenden.

Der Dienst KSN Proxy bietet folgende Möglichkeiten:

- Ein Benutzercomputer kann Anfragen an KSN ausführen und Informationen an KSN übertragen, auch wenn er keinen direkten Internetzugang besitzt.

- Der Dienst KSN Proxy übernimmt die Zwischenspeicherung von aufbereiteten Daten. Dadurch wird der Verbindungskanal zu dem externen Netzwerk entlastet und der Empfang angeforderter Informationen durch den Benutzercomputer wird beschleunigt.

Ausführliche Informationen über den Dienst KSN Proxy finden Sie in der *Hilfe zu Kaspersky Security Center*.

Verwendung von Kaspersky Security Network aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um die Verwendung von Kaspersky Security Network zu aktivieren oder zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Kaspersky Security Network** aus.
3. Verwenden Sie den Schalter des **Kaspersky Security Network**, um die Komponente zu aktivieren oder zu deaktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Endpoint Security die Erklärung zu Kaspersky Security Network an. Wenn Sie zustimmen, akzeptieren Sie die KSN-Nutzungsbedingungen.

   Kaspersky Endpoint Security verwendet standardmäßig den erweiterten KSN-Modus. Im *erweiterten KSN-Modus* überträgt Kaspersky Endpoint Security zusätzliche Daten an Kaspersky.
4. Deaktivieren Sie bei Bedarf den Schalter **Erweiterten KSN-Modus aktivieren**.
5. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verwendung des KSN aktiviert ist, verwendet Kaspersky Endpoint Security daher Informationen über die Reputation von Dateien, Webressourcen und Programmen, die vom Kaspersky Security Network empfangen werden.

Einschränkungen des Private KSN

Mit dem Private KSN (im Folgenden auch KPSN genannt) können Sie Ihre eigene lokale Reputationsdatenbank verwenden, um die Reputation von Objekten (Dateien oder Webadressen) zu überprüfen. Die Reputation eines Objekts, das der lokalen Reputationsdatenbank hinzugefügt wird, hat eine höhere Priorität als ein Objekt, das dem KSN/KPSN hinzugefügt wird. Stellen Sie sich zum Beispiel vor, Kaspersky Endpoint Security untersucht einen Computer und fordert die Reputation einer Datei im KSN/KPSN an. Wenn die Datei eine „nicht vertrauenswürdige“ Reputation in der lokalen Reputationsdatenbank, aber eine „vertrauenswürdige“ Reputation im KSN/KPSN hat, erkennt Kaspersky Endpoint Security die Datei als „nicht vertrauenswürdig“ und führt die für erkannte Bedrohungen definierten Maßnahmen durch.

In einigen Fällen fordert Kaspersky Endpoint Security jedoch möglicherweise nicht die Reputation eines Objekts im KSN/KPSN an. Wenn dies der Fall ist, empfängt Kaspersky Endpoint Security keine Daten aus der lokalen Reputationsdatenbank von KPSN. Kaspersky Endpoint Security fragt aus folgenden Gründen möglicherweise nicht nach der Reputation eines Objekts im KSN/KPSN:

- Kaspersky-Programme verwenden Offline-Reputationsdatenbanken. Offline-Reputationsdatenbanken wurden entwickelt, um die Ressourcen während des Betriebs von Kaspersky-Programmen zu optimieren und kritisch wichtige Objekte auf dem Computer zu schützen. Offline-Reputationsdatenbanken werden von Kaspersky-Experten auf der Grundlage von Daten aus dem Kaspersky Security Network erstellt. Kaspersky-Programme aktualisieren Offline-Reputationsdatenbanken mit Antiviren-Datenbanken des jeweiligen Programms. Wenn Offline-Reputationsdatenbanken Informationen über ein untersuchtes Objekt enthalten, fordert das Programm die Reputation dieses Objekts nicht vom KSN/KPSN an.

- Untersuchungsausnahmen (vertrauenswürdige Zone) werden in den Programmeinstellungen konfiguriert. Wenn dies der Fall ist, berücksichtigt der Antrag die Reputation des Objekts in der lokalen Reputationsdatenbank nicht.

- Das Programm verwendet Optimierungstechnologien für Untersuchungen wie iSwift oder iChecker oder speichert Reputationsanforderungen in KSN/KPSN. Wenn dies der Fall ist, fordert das Programm möglicherweise nicht die Reputation von zuvor untersuchten Objekten an.

- Um die Arbeitslast zu optimieren, untersucht das Programm Dateien in einem bestimmten Format und einer bestimmten Größe. Die Liste der relevanten Formate und Größenbeschränkungen werden von Kaspersky-Experten festgelegt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können auch Optimierungseinstellungen für Untersuchungen in der Programmoberfläche konfigurieren, z. B. für die Komponente Schutz vor bedrohlichen Dateien.

Cloud-Modus für die Schutzkomponenten aktivieren und deaktivieren

Cloud-Modus – Modus des Programms, in dem Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken verwendet. Das Funktionieren des Programms mit einer eingeschränkten Version der Antiviren-Datenbanken wird durch Kaspersky Security Network gewährleistet. Mithilfe der eingeschränkten Version der Antiviren-Datenbanken kann die Auslastung des Computer-Arbeitsspeichers etwa um die Hälfte reduziert werden. Wenn Sie nicht an Kaspersky Security Network teilnehmen oder der Cloud-Modus deaktiviert ist, lädt Kaspersky Endpoint Security die komplette Version der Antiviren-Datenbanken von den Kaspersky-Servern herunter.

Bei der Verwendung von Kaspersky Private Security Network ist die Funktionalität des Cloud-Modus ab Version von Kaspersky Private Security Network 3.0 verfügbar.

Um den Cloud-Modus für die Schutzkomponenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Schutz** → **Erweiterter Schutz** → **Kaspersky Security Network aus**.

3. Verwenden Sie den Schalter **Cloud-Modus aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen lädt Kaspersky Endpoint Security beim nächsten Update eine Light-Version oder Vollversion der Antiviren-Datenbanken herunter.

Falls die eingeschränkte Version der Antiviren-Datenbanken nicht verfügbar ist, schaltet Kaspersky Endpoint Security automatisch zur Verwendung der vollständigen Version der Antiviren-Datenbanken um.

Verbindung zum Kaspersky Security Network prüfen

Mögliche Gründe, warum keine Verbindung mit dem Kaspersky Security Network besteht:

- Sie nehmen nicht an Kaspersky Security Network teil.
- Ihr Computer ist nicht mit dem Internet verbunden.
- Der aktuelle Schlüsselstatus erlaubt keine Verbindung mit dem Kaspersky Security Network. Die Verbindung zu KSN kann beispielsweise aus folgenden Gründen nicht verfügbar sein:
  - Das Programm ist nicht aktiviert.
  - Die Lizenz oder das Abonnement ist abgelaufen.
  - Es gibt Probleme mit dem Lizenzschlüssel (z. B. der Schlüssel wurde der Liste der verbotenen Schlüssel hinzugefügt).

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Verbindung zum Kaspersky Security Network besteht:

Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Kaspersky Security Network**.

Das Fenster **Kaspersky Security Network** wird geöffnet, in dem Informationen über die Aktivität von Kaspersky Security Network angezeigt werden. Das Programm ruft die statistischen Daten zur KSN-Verwendung ab, wenn das Fenster **Kaspersky Security Network** geöffnet wird. Die globale Statistik über die Infrastruktur der Cloud-Dienste von Kaspersky Security Network und die Synchronisierungzeit werden nicht in Echtzeit aktualisiert.

Im linken Bereich des Fensters **Kaspersky Security Network** wird einer der folgenden Statuswerte für die Verbindung zwischen dem Computer und Kaspersky Security Network angezeigt:

- *Aktiviert.*

  Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security verwendet wird und die KSN-Server verfügbar sind.

- *Aktiviert. Mit Einschränkungen verfügbar*.

  Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security verwendet wird, die KSN-Server aber nicht verfügbar sind.

  KSN-Server können aus den folgenden Gründen nicht verfügbar sein:

  - Der KSN-Proxy-Dienst (ksnproxy) läuft auf dem Computer.
  - Die Firewall blockiert Port 13111.

  Wenn seit der letzten Synchronisierung mit den KSN-Servern mehr als 15 Minuten vergangen sind oder der Status *Unbekannt* angezeigt wird, erhält der Verbindungsstatus von Kaspersky Endpoint Security mit Kaspersky Security Network den Wert *Aktiviert. Nicht verfügbar*.

- *Deaktiviert*.

  Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security nicht verwendet wird.

Falls mit den Servern von Kaspersky Security Network keine Verbindung mehr wiederherstellt werden kann, sollten Sie sich an den Technischen Support oder an Ihren Dienstleister wenden.

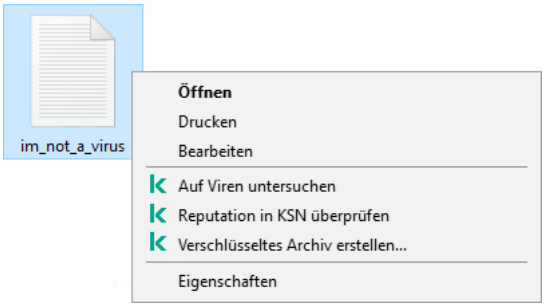
Reputation einer Datei in Kaspersky Security Network überprüfen

Wenn Sie an der Sicherheit einer Datei zweifeln, können Sie die Reputation in Kaspersky Security Network überprüfen.

Die Reputationsprüfung ist verfügbar, wenn Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben.

Um die Reputation einer Datei in Kaspersky Security Network zu überprüfen,

öffnen Sie das Kontextmenü der Datei und wählen Sie den Punkt **Reputation in KSN überprüfen** aus (s. Abb. unten).



Kontextmenü einer Datei

Kaspersky Endpoint Security zeigt die Reputation der Datei an:

Vertrauenswürdig. Die meisten Benutzer von Kaspersky Security Network haben bestätigt, dass die Datei vertrauenswürdig ist.

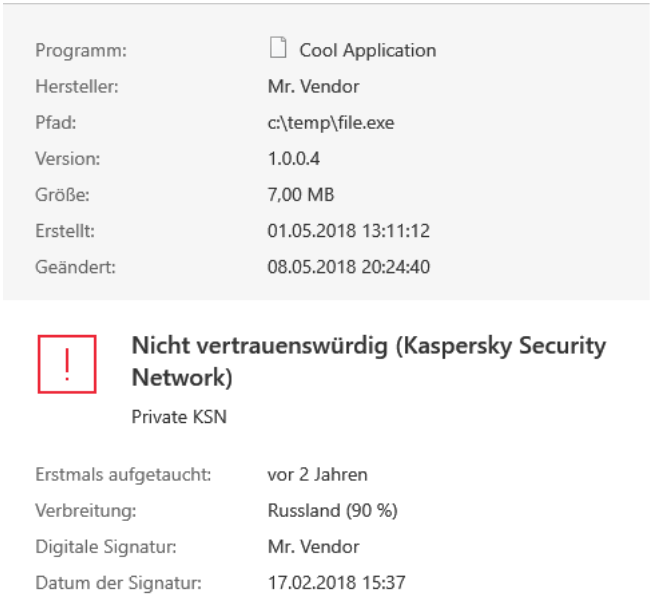
Legales Programm, mit dem Angreifer den Computer oder die Daten beschädigen können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Angreifern verwendet werden. Nähere Informationen zu legalen Programmen, die von Angreifern missbraucht werden können, um den Computer oder die Daten des Anwenders zu beschädigen, erhalten Sie auf der Website der Viren-Enzyklopädie von Kaspersky. Diese Programme können Sie zur Liste der vertrauenswürdigen Programme hinzufügen.

Nicht vertrauenswürdig. Virus oder anderes Programm, das eine Bedrohung darstellt.

Unbekannt. In Kaspersky Security Network liegen keine Informationen über die Datei vor. Sie können die Datei mithilfe der Antiviren-Datenbanken untersuchen (Punkt **Auf Viren untersuchen** im Kontextmenü).

Kaspersky Endpoint Security zeigt die KSN-Variante an, mit der die Reputation der Datei ermittelt wurde: *Global KSN* oder *Private KSN*.

Außerdem zeigt Kaspersky Endpoint Security zusätzliche Informationen über die Datei an (s. Abb. unten).



Reputation einer Datei in Kaspersky Security Network

Untersuchung verschlüsselter Verbindungen

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Nach der Installation fügt Kaspersky Endpoint Security dem Systemspeicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher) ein Kaspersky-Zertifikat hinzu. Kaspersky Endpoint Security umfasst auch die Verwendung der Systemspeicherung von vertrauenswürdigen Zertifikaten in Firefox und Thunderbird, um den Datenverkehr dieser Programme zu untersuchen.

Die Komponenten Web-Kontrolle, Schutz vor E-Mail-Bedrohungen und Schutz vor Web-Bedrohungen können den Netzwerkverkehr, der unter Verwendung der folgenden Protokolle über verschlüsselte Verbindungen übertragen wird, entschlüsseln und untersuchen:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Einstellungen der Untersuchung verschlüsselter Verbindungen anpassen

Um die Einstellungen für die Untersuchung verschlüsselter Verbindungen anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.

3. Wählen Sie im Abschnitt „Untersuchung verschlüsselter Verbindungen“ den Modus für die Untersuchung verschlüsselter Verbindungen aus:

   - **Verschlüsselte Verbindungen nicht untersuchen** Kaspersky Endpoint Security hat keinen Zugriff auf Inhalte von Websites, deren Adressen mit `https://` beginnen.

   - **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor bedrohlichen Dateien“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ angefordert wird.

   - **Verschlüsselte Verbindungen immer untersuchen** Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind.

   Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.

4. Fügen Sie falls erforderlich Untersuchungsausnahmen hinzu: vertrauenswürdige Adressen und Programme.

5. Klicken Sie auf **Erweiterte Einstellungen**.

6. Passen Sie die Einstellungen für die Untersuchung verschlüsselter Verbindungen an (siehe folgende Tabelle).

7. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für die Untersuchung verschlüsselter Verbindungen

Einstellung	Beschreibung
Beim Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat	• **Erlauben**. Ist diese Variante ausgewählt und es erfolgt ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat, so erlaubt Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite enthält eine Warnung und Informationen über den Grund, aus welchem ein Besuch dieser Domäne als riskant gilt. Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. Nach Klick auf diesen Link zeigt Kaspersky Endpoint Security eine Stunde lang keine Warnungen über ein nicht vertrauenswürdiges Zertifikat an, wenn zu anderen Ressourcen in derselben Domäne gewechselt wird. • **Verbindung blockieren** Ist diese Variante ausgewählt und es erfolgt ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat, so blockiert Kaspersky Endpoint Security die Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite informiert über den Grund, aus dem der Wechsel zu dieser Domäne blockiert wurde.

Beim Auftreten von Fehlern bei der Untersuchung verschlüsselter Verbindungen	• **Verbindung blockieren** Wenn dieses Element ausgewählt wurde und bei der Untersuchung einer geschützten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security diese Netzwerkverbindung. • **Domäne zu Ausnahmen hinzufügen**. Wenn dieses Element ausgewählt ist und bei der Untersuchung einer geschützten Verbindung ein Fehler auftritt, so fügt Kaspersky Endpoint Security die betreffende Domäne zu einer Liste der Domänen mit Untersuchungsfehlern hinzu und kontrolliert den verschlüsselten Netzwerkverkehr beim Wechsel zu dieser Domäne nicht. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich. Um den Inhalt der Liste zurückzusetzen, wählen Sie das Element **Verbindung blockieren** aus.
Verbindungen über das Protokoll SSL 2.0 blockieren	Ist das Kontrollkästchen aktiviert, so blockiert Kaspersky Endpoint Security die Netzwerkverbindungen, die über das Protokoll SSL 2.0 hergestellt werden. Ist das Kontrollkästchen deaktiviert, so blockiert Kaspersky Endpoint Security die Netzwerkverbindungen, die über das SSL 2.0-Protokoll hergestellt werden, nicht und überwacht den Netzwerkverkehr, der über diese Verbindungen übertragen wird, nicht.
Geschützte Verbindung mit einer Website, die ein EV-Zertifikat verwendet, entschlüsseln	EV-Zertifikate (eng. Extended Validation Certificate) bestätigen die Authentizität von Websites und erhöhen die Sicherheit einer Verbindung. Die Browser informieren durch ein Schloss-Symbol in der Adressleiste darüber, ob eine Website ein EV-Zertifikat hat. Außerdem kann die Adressleiste des Browsers vollständig oder teilweise grüne Farbe besitzen. Ist das Kontrollkästchen aktiviert, so entschlüsselt und überwacht Kaspersky Endpoint Security die geschützten Verbindungen, die ein EV-Zertifikat verwenden. Ist das Kontrollkästchen deaktiviert, so hat Kaspersky Endpoint Security keinen Zugriff auf den Inhalt des HTTPS-Datenverkehrs. Deshalb kontrolliert das Programm den HTTPS-Datenverkehr nur nach der Adresse einer Website, z. B. `https://facebook.com`. Wenn Sie eine Website mit einem EV-Zertifikat zum ersten Mal öffnen, wird die verschlüsselte Verbindung unabhängig davon entschlüsselt, ob das Kontrollkästchen aktiviert ist oder nicht.

Untersuchung verschlüsselter Verbindungen in Firefox und Thunderbird

Nach der Installation fügt Kaspersky Endpoint Security dem Systemspeicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher) ein Kaspersky-Zertifikat hinzu. Standardmäßig verwenden Firefox und Thunderbird ihren eigenen proprietären Mozilla-Zertifikatspeicher anstelle des Windows-Zertifikatspeichers. Wenn das Kaspersky Security Center in Ihrem Unternehmen installiert ist und eine Richtlinie auf einen Computer angewendet wird, ermöglicht Kaspersky Endpoint Security automatisch die Verwendung des Windows-Zertifikatspeichers in Firefox und Thunderbird, um den Datenverkehr dieser Programme zu untersuchen. Wenn eine Richtlinie nicht auf den Computer angewendet wird, können Sie den Zertifikatspeicher wählen, der von Mozilla-Programmen verwendet wird. Wenn Sie den Mozilla-Zertifikatspeicher ausgewählt haben, fügen Sie ihm manuell ein Kaspersky-Zertifikat hinzu. Dies hilft, Fehler bei der Arbeit mit HTTPS-Verkehr zu vermeiden.

Um den Datenverkehr im Browser „Mozilla Firefox“ und im E-Mail-Client „Thunderbird“ zu untersuchen, müssen Sie die Untersuchung verschlüsselter Verbindungen aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, untersucht Kaspersky Endpoint Security den Datenverkehr im Browser „Mozilla Firefox“ und im E-Mail-Client „Thunderbird“ nicht.

Bevor Sie ein Zertifikat zum Mozilla-Speicher hinzufügen, exportieren Sie das Kaspersky-Zertifikat über die Windows-Systemsteuerung (Browsereigenschaften). Einzelheiten zum Export des Kaspersky-Zertifikats finden Sie in der Wissensdatenbank des Technischen Supports. Einzelheiten zum Hinzufügen eines Zertifikats zur Speicherung finden Sie auf der *Website zur technischen Unterstützung von Mozilla*.

Sie können den Zertifikatspeicher nur in der lokalen Benutzeroberfläche des Programms auswählen.

So wählen Sie einen Zertifikatspeicher zum Untersuchen verschlüsselter Verbindungen in Firefox und Thunderbird:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Aktivieren Sie im Block **Mozilla Firefox und Thunderbird** das Kontrollkästchen **Sicheren Datenverkehr in Mozilla-Programmen untersuchen**.
4. Wählen Sie einen Zertifikatspeicher aus:
   - **Windows-Zertifikatspeicher verwenden**. Das Kaspersky-Stammzertifikat wird zu diesem Speicher hinzugefügt, während Kaspersky Endpoint Security installiert wird.
   - **Zertifikatspeicher von Mozilla verwenden**. Mozilla Firefox und Thunderbird verwenden ihre eigenen Zertifikatspeicher. Wenn der Mozilla-Zertifikatspeicher ausgewählt ist, müssen Sie das Kaspersky-Stammzertifikat in den Browser-Eigenschaften manuell zu diesem Speicher hinzufügen.
5. Speichern Sie die vorgenommenen Änderungen.

Geschütze Verbindungen von der Untersuchung ausschließen

Die meisten Web-Ressourcen verwenden geschützte Verbindungen. Die Kaspersky-Experten empfehlen, die Untersuchung verschlüsselter Verbindungen zu aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen Sie bei der Arbeit stört, können Sie die entsprechende Website als Ausnahme zu den *vertrauenswürdigen Adressen* hinzufügen. Wenn ein vertrauenswürdiges Programm eine geschützte Verbindung verwendet, können Sie die Untersuchung verschlüsselter Verbindungen für dieses Programm deaktivieren. Sie können die Untersuchung verschlüsselter Verbindungen beispielsweise für Cloud-Speicher-Programme deaktivieren, da solche Programme eine Zwei-Faktor-Authentifikation mit einem eigenen Zertifikat verwenden.

Um eine Webadresse von der Untersuchung verschlüsselter Verbindungen auszuschließen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Vertrauenswürdige Adressen**.
4. Klicken Sie auf **Hinzufügen**.

5. Geben Sie einen Domänennamen oder eine IP-Adresse ein, damit das Programm Kaspersky Endpoint Security die geschützten Verbindungen nicht untersucht, die beim Wechsel zu dieser Webseite hergestellt werden.

   Kaspersky Endpoint Security unterstützt das Symbol `*` bei der Eingabe eines Domänennamens.

   > Kaspersky Endpoint Security unterstützt keine Masken für IP-Adressen.

   Beispiele:

   - `domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Diese Angabe schließt Subdomänen aus (z. B. `subdomain.domain.com`).
   - `subdomain.domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Diese Angabe schließt die Domäne `domain.com` aus.
   - `*.domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://movies.domain.com`, `https://images.domain.com/page123`. Diese Angabe schließt die Domäne `domain.com` aus.

6. Speichern Sie die vorgenommenen Änderungen.

Geschützte Verbindungen, bei denen Fehler auftreten, werden von Kaspersky Endpoint Security standardmäßig nicht untersucht und die Website wird zur Liste *Domänen mit Untersuchungsfehlern* hinzugefügt. Kaspersky Endpoint Security erstellt für jeden Benutzer eine separate Liste und überträgt diese Daten nicht an Kaspersky Endpoint Security. Sie können das Blockieren einer Verbindung beim Auftreten eines Fehlers aktivieren. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich.

- Speichern Sie die vorgenommenen Änderungen.

Geschützte Verbindungen, bei denen Fehler auftreten, werden von Kaspersky Endpoint Security standardmäßig nicht untersucht und die Website wird zur Liste *Domänen mit Untersuchungsfehlern* hinzugefügt. Kaspersky Endpoint Security erstellt für jeden Benutzer eine separate Liste und überträgt diese Daten nicht an Kaspersky Endpoint Security. Sie können das Blockieren einer Verbindung beim Auftreten eines Fehlers aktivieren. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich.

Um die Liste der Domänen mit Untersuchungsfehlern anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Klicken Sie im Abschnitt **Untersuchung verschlüsselter Verbindungen** auf die Schaltfläche **Domänen mit Untersuchungsfehlern**.

   Die Liste der Domänen mit Untersuchungsfehlern wird geöffnet. Um die Liste zurückzusetzen, müssen Sie in der Richtlinie das Blockieren einer Verbindung beim Auftreten eines Fehlers aktivieren, die Richtlinie anwenden, die Einstellung auf den ursprünglichen Zustand zurücksetzen und die Richtlinie erneut anwenden.

Die Kaspersky-Experten pflegen eine Liste mit vertrauenswürdigen Websites, die Kaspersky Endpoint Security unabhängig von den Programmeinstellungen nicht untersucht. Dies sind die *globalen Ausnahmen*.

Um die globalen Ausnahmen für die Untersuchung des geschützten Datenverkehrs einzusehen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.

3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Websites**.

   Dies öffnet eine Liste von Websites, die von Kaspersky-Experten zusammengestellt wurde. Kaspersky Endpoint Security überprüft geschützte Verbindungen nicht auf Websites auf der Liste. Die Tabelle wird beim Update der Datenbanken und Module von Kaspersky Endpoint Security aktualisiert.

Web-Kontrolle

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch lässt sich Datenverkehr einsparen und die zweckentfremdete Nutzung der Arbeitszeit reduzieren. Wenn ein Benutzer versucht, eine Website zu öffnen, auf den die „Web-Kontrolle“ den Zugriff beschränkt, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).

Kaspersky Endpoint Security kontrolliert nur den HTTP- und HTTPS-Datenverkehr.

Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

Methoden zur Verwaltung des Zugriffs auf Websites

Mithilfe der „Web-Kontrolle“ kann der Zugriff auf Websites wie folgt angepasst werden:

- **Website-Kategorie**. Eine Kategorisierung der Websites wird gewährleistet vom Cloud-Dienst für Kaspersky Security Network, von der heuristischen Analyse und von der Datenbank für unbekannte Websites (im Lieferumfang des Programms enthalten). So können Sie z. B. den Benutzerzugriff auf die Kategorie „Soziale Netzwerke“ oder auf andere Kategorien beschränken.
- **Datentyp**. Sie können für Benutzer den Zugriff auf die Daten auf einer Website beschränken und beispielsweise Grafiken verbergen. Kaspersky Endpoint Security ermittelt den Datentyp aufgrund des Dateiformats, nicht nach der Erweiterung.

  Dateien in Archiven werden durch Kaspersky Endpoint Security nicht untersucht. Befinden sich beispielsweise Bilddateien in einem Archiv, so ermittelt Kaspersky Endpoint Security den Datentyp „Archive“, nicht „Bilddateien“.

- **Bestimmte Adresse**. Sie können eine Webadresse eingeben oder Masken verwenden.

Sie können gleichzeitig mehrere Methoden verwenden, um den Zugriff auf Websites zu regulieren. Der Zugriff auf den Datentyp „Dateien für Office-Programme“ lässt sich beispielsweise nur für die Website-Kategorie „Web-E-Mail“ beschränken.

Regeln für den Zugriff auf Websites

Die „Web-Kontrolle“ verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Sie können eine Regel für den Zugriff auf Websites wie folgt zusätzlich anpassen:

- Benutzer, für welche die Regel gilt.

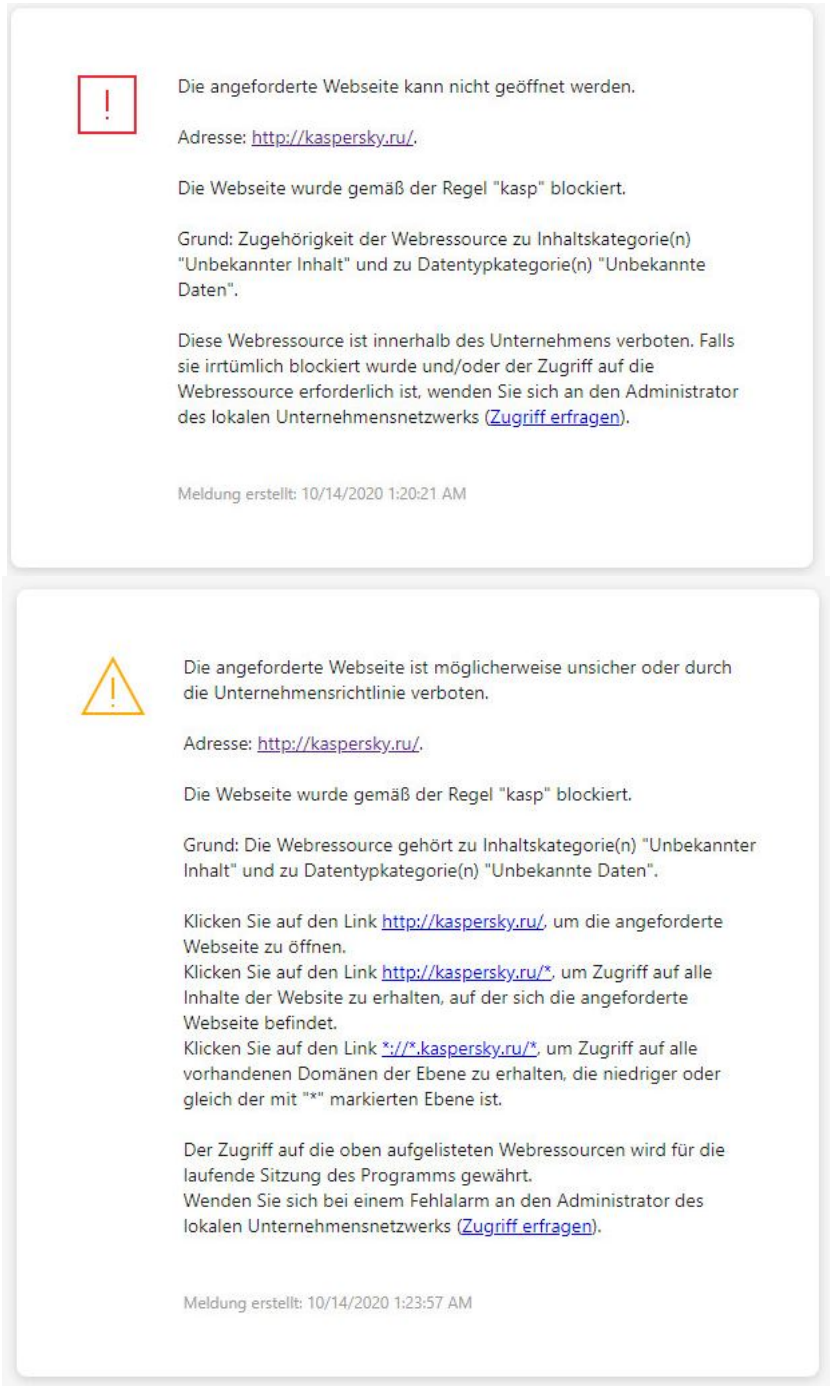
  Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- Zeitplan für die Regel.

  Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Prioritäten für Zugriffsregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Website in mehreren Regeln vorkommt, reguliert die „Web-Kontrolle“ den Zugriff auf die Website nach der Regel mit der höchsten Priorität. Es kann beispielsweise vorkommen, dass Kaspersky Endpoint Security ein Unternehmensportal als soziales Netzwerk betrachtet. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „Soziale Netzwerke“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Unternehmens-Web-Portal muss eine höhere Priorität haben als die Zugriffsregel für soziale Netzwerke.



Benachrichtigungen der „Web-Kontrolle"

Web-Kontrolle aktivieren und deaktivieren

Die Web-Kontrolle ist standardmäßig aktiviert.

Um die Web-Kontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Web-Kontrolle**.
3. Verwenden Sie den Schalter **Web-Kontrolle**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Aktionen für die Zugriffsregeln für Webressourcen

Es wird davon abgeraten, mehr als 1.000 Zugriffsregeln für Webressourcen zu erstellen, da es andernfalls zu Systeminstabilität kommen kann.

Eine Zugriffsregel für Webressourcen besteht aus einer Auswahl von Filtern und aus einer Aktion, die Kaspersky Endpoint Security ausführt, wenn ein Benutzer die in der Regel beschriebenen Webressourcen zur im Regelzeitplan festgelegten Zeit besucht. Mithilfe von Filtern kann der Bereich der Webressourcen genau festgelegt werden, auf die der Zugriff durch die Komponente „Web-Kontrolle“ kontrolliert wird.

Folgende Filter sind verfügbar:

- **Inhaltsfilter**. Die Web-Kontrolle unterteilt die Webressourcen nach Inhaltskategorien und Datentypkategorien. Sie können den Zugriff der Benutzer auf jene Daten kontrollieren, die sich in Webressourcen befinden, welche zu den durch diese Kategorien definierten Datentypen gehören. Wenn ein Benutzer Webressourcen besucht, die zu einer gewählten Inhaltskategorie und / oder Datentypkategorie gehören, führt Kaspersky Endpoint Security die in der Regel festgelegte Aktion aus.

- **Filter für Adressen von Webressourcen**. Sie können den Zugriff der Benutzer auf alle Adressen von Webressourcen oder auf bestimmte Adressen von Webressourcen und / oder Adressgruppen von Webressourcen kontrollieren.

  Wenn die Filterung nach Inhalt und die Filterung nach Web-Ressourcenadressen angegeben ist und die angegebenen Web-Ressourcenadressen und/oder Gruppen von Web-Ressourcenadressen zu den ausgewählten Inhaltskategorien oder Datentypkategorien gehören, kontrolliert Kaspersky Endpoint Security nicht den Zugriff auf alle Web-Ressourcen in den ausgewählten Inhaltskategorien und/oder Datentypkategorien. Stattdessen kontrolliert das Programm nur den Zugriff auf die angegebenen Web-Ressourcenadressen und/oder Gruppen von Web-Ressourcenadressen.

- **Filter für Namen von Benutzern und Benutzergruppen**. Sie können Benutzer und / oder Benutzergruppen festlegen, für die der Zugriff auf Webressourcen nach der Regel kontrolliert werden soll.

- **Zeitplan für die Regel**. Sie können einen Zeitplan für die Regel erstellen. Der Zeitplan für eine Regel bestimmt die Zeit, in der Kaspersky Endpoint Security den Zugriff auf die in einer Regel festgelegten Webressourcen kontrolliert.

Nach der Installation von Kaspersky Endpoint Security ist die Regelliste der Komponente „Web-Kontrolle“ nicht leer. Es sind zwei Regeln vordefiniert:

- Regel „Skripte und Stylesheets“, die allen Benutzern jederzeit den Zugriff auf alle Webressourcen erlaubt, in deren Adressen Dateinamen mit der Endung CSS, JS, oder VBS vorkommen. Beispiele: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- Standardregel. Abhängig von der ausgewählten Aktion erlaubt oder verbietet diese Regel allen Benutzern den Zugriff auf alle Webressourcen, die nicht unter andere Regeln fallen.

Hinzufügen einer Web-Ressourcen-Zugriffsregel

Gehen Sie folgendermaßen vor, um eine Regel für den Zugriff auf Webressourcen hinzuzufügen oder zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Web-Kontrolle**.
3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.
4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.
5. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.
6. Wählen Sie den Status **Aktiv** für die Web-Ressourcen-Zugriffsregel.

   Sie können die Web-Ressourcen-Zugriffsregel jederzeit mit dem Schalter deaktivieren.
7. Wählen Sie im Bock **Aktion** die entsprechende Option:

   - **Erlauben**. Wenn dieser Wert gewählt wird, erlaubt Kaspersky Endpoint Security den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Blockieren** Wenn dieser Wert gewählt wird, verbietet Kaspersky Endpoint Security den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Warnen**. Ist dieser Wert gewählt, so warnt Kaspersky Endpoint Security bei einem Zugriffsversuch auf Webressourcen, welche dieser Regel entsprechen, vor dem Besuch der Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.
8. Wählen Sie im Block **Filtertyp** den entsprechenden Inhaltsfilter aus:

   - **Nach Inhaltskategorien**. Sie können den Benutzerzugriff auf Web-Ressourcen nach Kategorie steuern (z. B. die Kategorie *Soziale Netzwerke*).
   - **Nach Datentypen**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Grafiken*) steuern.

   So konfigurieren Sie den Inhaltsfilter:

   a. Klicken Sie auf den Link **Anpassen**.

   b. Aktivieren Sie die Kontrollkästchen für die entsprechenden Inhaltskategorien und/oder Datentypen.

   Ist das Kontrollkästchen für eine Inhaltskategorie und/oder einen Datentyp aktiviert, so verwendet Kaspersky Endpoint Security die Regel, um den Zugriff auf die Webressourcen zu kontrollieren, die den gewählten Inhaltskategorien und/oder Dateitypen angehören.

   c. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.
9. Wählen Sie im Block **Adressen** den entsprechenden Adressenfilter für Webressourcen aus:

   - **Auf alle Adressen**. Web-Kontrolle filtert Web-Ressourcen nicht nach Adressen.
   - **Auf bestimmte Adressen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. So erstellen Sie eine Liste mit Adressen von Webressourcen:

     a. Klicken Sie auf die Schaltfläche **Adresse hinzufügen** oder **Adressgruppe hinzufügen**.

b. Erstellen Sie im geöffneten Fenster eine Liste mit Adressen von Webressourcen. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren.

c. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, ist für das https-Protokoll nur die Filterung nach dem Servernamen verfügbar.

10. Wählen Sie im Block **Benutzer** den entsprechenden Filter für Benutzer aus:

- **Auf alle Benutzer**. Web-Kontrolle filtert keine Web-Ressourcen für bestimmte Benutzer.
- **An einzelne Benutzer und/oder Gruppen**. Web-Kontrolle filtert Web-Ressourcen nur für bestimmte Benutzer. So erstellen Sie eine Liste der Benutzer, auf die Sie die Regel anwenden möchten:

  a. Klicken Sie auf **Hinzufügen**.

  b. Wählen Sie im geöffneten Fenster die Benutzer oder Benutzergruppen aus, auf die Sie die Web-Ressourcen-Zugriffsregel anwenden möchten.

  c. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

11. Wählen Sie entweder aus der Dropdown-Liste **Zeitplan für die Regel** den Namen des entsprechenden Zeitplans oder erstellen Sie auf Basis des gewählten Regelzeitplans einen neuen Zeitplan. Gehen Sie dazu folgendermaßen vor:

  a. Klicken Sie auf die Schaltfläche **Zeitplanverwaltung**.

  b. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

  c. Geben Sie in dem geöffneten Fenster den Namen des Regelzeitplans ein.

  d. Konfigurieren Sie den Zeitplan für den Zugriff auf die Web-Ressource für Benutzer.

  e. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

12. Speichern Sie die vorgenommenen Änderungen.

Zugriffsregeln für Webressourcen eine Priorität zuweisen

Sie können jeder Regel aus der Liste eine bestimmte Priorität zuweisen, indem Sie die Regeln entsprechend anordnen.

Gehen Sie folgendermaßen vor, um Regeln für den Zugriff auf Webressourcen eine Priorität zuzuweisen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Web-Kontrolle**.
3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

4. Wählen Sie im geöffneten Fenster die Regel aus, deren Priorität Sie ändern möchten.

5. Verwenden Sie die Schaltflächen **Aufwärts** und **Abwärts**, um die Regel an die entsprechende Position in der Liste der Zugriffsregeln für Webressourcen zu verschieben.

6. Speichern Sie die vorgenommenen Änderungen.

Zugriffsregel für Webressourcen aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um eine Zugriffsregel für Webressourcen zu aktivieren oder zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Web-Kontrolle**.

3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

4. Wählen Sie im geöffneten Fenster die Regel aus, die Sie aktivieren oder deaktivieren möchten.

5. Gehen Sie in der Spalte **Status** wie folgt vor:

   - Wählen Sie den Wert **Aktiv**, um die Verwendung einer Regel zu aktivieren.

   - Wählen Sie den Wert **Inaktiv**, um die Verwendung einer Regel zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und importieren der Liste vertrauenswürdiger Webadressen

Sie können die Liste der Regeln der Web-Richtlinienverwaltung in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie die Liste der Regeln der Web-Richtlinienverwaltung sichern oder die Liste auf einen anderen Server migrieren.

So exportieren und importieren Sie eine Liste von Regeln der Web-Richtlinienverwaltung in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Sicherheitskontrollen → Web-Richtlinienverwaltung** aus.
6. So exportieren Sie die Liste der Regeln für die Web-Richtlinienverwaltung:
   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
7. So importieren Sie die Liste der Regeln für die Web-Richtlinienverwaltung:
   a. Klicken Sie auf **Import**.
      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste von Regeln der Web-Richtlinienverwaltung in der Web Console und der Cloud Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste der Regeln exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrollen** → **Web-Richtlinienverwaltung**.
5. Um die Liste der Regeln zu exportieren, gehen Sie im Block **Liste der Regeln** wie folgt vor:
   a. Wählen Sie die Regeln, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Regeln exportieren möchten, oder exportieren Sie die gesamte Liste.
   d. Klicken Sie auf **Export**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine XML-Datei im Standard-Download-Ordner.
6. Zum Importieren der Liste der Regeln gehen Sie im Block **Liste der Regeln** wie folgt vor:
   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

Zugriffsregeln für Webressourcen testen

Sie können die Regeln der Web-Kontrolle bewerten, um festzustellen, inwieweit sie aufeinander abgestimmt sind. Dazu dient in der Komponente „Web-Kontrolle“ die Funktion „Regeldiagnose“.

Gehen Sie folgendermaßen vor, um die Regeln für den Zugriff auf Webressourcen zu testen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Web-Kontrolle**.
3. Klicken Sie im Block **Einstellungen** auf den Link **Regeldiagnose**.

   Das Fenster **Regeldiagnose** wird geöffnet.

4. Wenn Sie die Regeln testen möchten, die Kaspersky Endpoint Security zur Steuerung des Zugriffs auf eine bestimmte Web-Ressource verwendet, aktivieren Sie das Kontrollkästchen **Geben Sie eine Adresse an**. Geben Sie die Adresse der Web-Ressource in das unten stehende Feld ein.

5. Erstellen Sie eine Liste der Benutzer und/oder Benutzergruppen, um die Regeln zu überprüfen, nach denen Kaspersky Endpoint Security den Zugriff auf Webressourcen für bestimmte Benutzer und/oder Benutzergruppen kontrolliert.

6. Wenn Sie die Regeln testen möchten, die Kaspersky Endpoint Security zur Steuerung des Zugriffs auf Webressourcen bestimmter Inhaltskategorien und/oder Datentyp-Kategorien verwendet, aktivieren Sie das Kontrollkästchen **Inhalt filtern** und wählen Sie die entsprechende Option aus der Dropdown-Liste (**Nach Inhaltskategorien**, **Nach Datentypen** oder **Nach Inhaltskategorien und Datentypen**).

7. Aktivieren Sie das Kontrollkästchen **Zeitpunkt des Zugriffsversuchs berücksichtigen**, wenn bei der Regelprüfung der Zeitpunkt (Wochentag und Uhrzeit) berücksichtigt werden soll, zu dem ein Zugriffsversuch auf die Webressourcen erfolgt, die in den Bedingungen für die Regeldiagnose festgelegt wurden. Geben Sie nun einen Wochentag und eine Uhrzeit an.

8. Klicken Sie auf die Schaltfläche **Prüfen**.

Nach der Überprüfung wird eine Meldung über die Aktion angezeigt, die Kaspersky Endpoint Security bei einem Zugriffsversuch auf die angegebene Webressource in Übereinstimmung mit der zuerst ausgelösten Regel ausführen würde (Erlaubnis, Verbot, Warnung). Die zuerst ausgelöste Regel ist jene Regel, die in der Regelliste der Web-Kontrolle unter jenen Regeln, welche die Diagnosebedingungen erfüllen, an erster Stelle steht. Die Meldung wird rechts von der Schaltfläche **Prüfen** angezeigt. Die darunter angezeigte Tabelle enthält eine Liste der übrigen ausgelösten Regeln mit Angabe der Aktion, die Kaspersky Endpoint Security ausführt. Die Regeln sind in absteigender Reihenfolge nach der Priorität angeordnet.

Adressliste für Webressourcen exportieren und importieren

Wenn Sie in einer Zugriffsregel bereits eine Adressliste für Webressourcen angelegt haben, kann die Liste in eine txt-Datei exportiert werden. Die Liste kann später aus dieser Datei importiert werden, um beim Anpassen von Regeln keine neue Adressliste für Webressourcen manuell erstellen zu müssen. Die Möglichkeit zum Export und Import einer Adressliste für Webressourcen ist beispielsweise vorteilhaft, wenn Sie Regeln mit ähnlichen Einstellungen erstellen möchten.

Gehen Sie folgendermaßen vor, um eine Adressliste für Webressourcen zu importieren oder zu exportieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Web-Kontrolle**.

3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

4. Wählen Sie die Regel, deren Adressliste für Webressourcen exportiert oder importiert werden soll.

5. Um die Liste der vertrauenswürdigen Webadressen zu exportieren, gehen Sie im Block **Adressen** wie folgt vor:

   a. Wählen Sie die Adressen aus, die Sie exportieren möchten.

      Wenn Sie keine Adresse ausgewählt haben, exportiert Kaspersky Endpoint Security alle Adressen.

   b. Klicken Sie auf **Export**.

c. Geben Sie im geöffneten Fenster den Namen der TXT-Datei ein, in die Sie die Liste der Webressourcen-Adressen exportieren möchten, und wählen Sie den Ordner, in dem Sie diese Datei speichern möchten.

d. Klicken Sie auf **Speichern**.

Kaspersky Endpoint Security exportiert die Liste der Adressen von Webressourcen in eine TXT-Datei.

6. Um die Liste der Webressourcen zu importieren, gehen Sie im Block **Adressen** wie folgt vor:

a. Klicken Sie auf **Import**.

Wählen Sie in dem sich öffnenden Fenster die TXT-Datei aus, aus der Sie die Liste der Webressourcen importieren möchten.

b. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der TXT-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Überwachung der Internetaktivitäten von Benutzern

Kaspersky Endpoint Security erlaubt es, Daten über den Besuch aller Websites zu protokollieren, einschließlich erlaubter Websites. So können Sie einen vollständigen Verlauf aller im Browser besuchten Websites erhalten. Kaspersky Endpoint Security sendet Ereignisse über die Benutzeraktivitäten an Kaspersky Security Center, an den lokalen Bericht für Kaspersky Endpoint Security, an das Windows-Ereignisprotokoll. Um in Kaspersky Security Center Ereignisse zu erhalten, müssen die Ereigniseinstellungen in der Verwaltungskonsole oder in „Web Console“ angepasst werden. Sie können außerdem festlegen, dass „Web-Kontrolle“-Ereignisse per E-Mail gesendet werden und Benachrichtigungen auf dem Bildschirm des Benutzercomputers angezeigt werden.

Kaspersky Endpoint Security erstellt die folgenden Ereignisse über die Internetaktivitäten des Benutzers:

- Sperrung einer Website (Status *Kritische Ereignisse*);
- Besuch einer nicht empfohlenen Website (Status *Warnung*);
- Besuch einer erlaubten Website (Status *Informative Meldungen*).

Bevor Sie die Überwachung der Internet-Aktivitäten der Benutzer aktivieren, müssen Sie Folgendes tun:

- Fügen Sie ein Webseiten-Interaktionsskript in den Webverkehr ein (siehe die Anweisungen unten). Das Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen.
- Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

So injizieren Sie ein Webseiten-Interaktionsskript in den Webverkehr:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Aktivieren Sie im Block **Verkehrsverarbeitung** das Kontrollkästchen **Interaktionsskript in Verkehr injizieren**.
4. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen wird Kaspersky Endpoint Security ein Skript zur Interaktion mit Webseiten in den Web-Datenverkehr injizieren. Dieses Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen für die Ereignisanzeige des Programms, die Ereignisanzeige des Betriebssystems und Berichte.

Um die Protokollierung von „Web-Kontrolle"-Ereignissen auf dem Benutzercomputer anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster „Einstellungen" den Abschnitt **Benutzeroberfläche**.
3. Klicken Sie im Block **Benachrichtigungen** auf die Schaltfläche **Benachrichtigungsregeln**.
4. Wählen Sie im folgenden Fenster den Abschnitt **Web-Kontrolle** aus.

   Eine Tabelle der „Web-Kontrolle"-Ereignisse und Benachrichtigungsmethoden wird geöffnet.
5. Passen Sie für jedes Ereignis eine Benachrichtigungsmethode an: **In lokalem Bericht speichern** und **Im Windows-Ereignisprotokoll speichern**.

   Damit Ereignisse protokolliert werden, die sich auf den Besuch erlaubter Websites beziehen, muss die „Web-Kontrolle" zusätzlich angepasst werden (s. Anleitung unten).

   In der Ereignistabelle können Sie außerdem eine Bildschirmbenachrichtigung und eine E-Mail-Benachrichtigung aktivieren. Für den Versand von E-Mail-Benachrichtigungen müssen die Einstellungen des SMTP-Servers angepasst werden. Details über den Versand von E-Mail-Benachrichtigungen finden Sie in der *Hilfe zu Kaspersky Security Center*.
6. Speichern Sie die vorgenommenen Änderungen.

Künftig protokolliert Kaspersky Endpoint Security die Ereignisse über die Internetaktivitäten des Benutzers.

Die „Web-Kontrolle" sendet Ereignisse, welche die Benutzeraktivität betreffen, wie folgt an Kaspersky Security Center:

- Wenn Sie Kaspersky Security Center verwenden, sendet die „Web-Kontrolle" Ereignisse über alle Objekte, aus denen eine Webseite besteht. Deshalb kann es sein, dass bei der Sperrung einer Webseite mehrere Ereignisse erstellt werden. Beispiel: Bei der Sperrung der Webseite http://www.example.com kann Kaspersky Endpoint Security Ereignisse über die folgenden Objekt senden: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js und so weiter.
- Wenn Sie Kaspersky Security Center Cloud Console verwenden, gruppiert die „Web-Kontrolle" die Ereignisse und sendet nur das Protokoll und die Domäne der Webseite. Wenn der Benutzer beispielsweise die nicht empfohlenen Webseiten http://www.example.com/main, http://www.example.com/contact und http://www.example.com/gallery besucht hat, sendet Kaspersky Endpoint Security nur ein Ereignis für das Objekt http://www.example.com.

Um die Protokollierung von Ereignissen über den Besuch erlaubter Websites zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Web-Kontrolle**.
3. Klicken Sie im Block **Zusätzlich** auf die Schaltfläche **Erweiterte Einstellungen**.
4. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Daten über den Besuch erlaubter Seiten protokollieren**.

5. Speichern Sie die vorgenommenen Änderungen.

Künftig können Sie einen vollständigen Verlauf aller im Browser besuchten Websites einsehen.

Meldungsvorlagen für die Web-Kontrolle ändern

Abhängig davon, welche Aktion in den Eigenschaften der Regeln für die Web-Kontrolle festgelegt ist, zeigt Kaspersky Endpoint Security beim Versuch eines Benutzers, Zugriff auf Webressourcen zu erhalten, eine Meldung an (die Antwort des HTTP-Servers wird durch eine HTML-Seite mit einer Meldung ersetzt). Folgende Meldungstypen sind möglich:

- Warnmeldung. Eine solche Meldung warnt den Benutzer, dass vom Besuch einer Webressource abgeraten wird und/oder der Besuch gegen die Sicherheitsrichtlinie des Unternehmens verstößt. Kaspersky Endpoint Security zeigt eine Warnmeldung an, wenn in den Einstellungen der Regel, welche diese Webressource beschreibt, in der Dropdown-Liste **Aktion** das Element **Warnen** gewählt ist.

  Hält der Benutzer die Warnung für einen Irrtum, so kann der Benutzer mit einem Link aus der Warnung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

- Meldung über die Sperrung einer Webressource. Kaspersky Endpoint Security zeigt eine Meldung über die Sperrung einer Webressource an, wenn in den Einstellungen der Regel, welche diese Webressource beschreibt, in der Dropdown-Liste **Aktion** das Element **Verbieten** gewählt ist.

  Hält der Benutzer die Zugriffssperre auf eine Webressource für einen Irrtum, so kann der Benutzer mit einem Link aus der Sperrmeldung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

Für die Warnmeldung, für die Meldung über die Sperrung einer Webressource und für die Nachricht an den Administrator des lokalen Unternehmensnetzwerks sind Vorlagen vorgesehen. Der Inhalt dieser Vorlagen kann geändert werden.

Gehen Sie folgendermaßen vor, um die Meldungsvorlage für die Web-Kontrolle zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Web-Kontrolle**.

3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Web-Kontrolle:

   - **Warnungen**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt.

   - **Sperrung**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert.

   - **Nachricht an den Administrator**. Das Eingabefeld enthält eine Vorlage für die Meldung, die an den Administrator des lokalen Firmennetzwerks zu senden ist, wenn der Zugriff auf eine Webressource nach Meinung des Benutzers irrtümlich blockiert wurde.

4. Speichern Sie die vorgenommenen Änderungen.

Regeln für das Erstellen von Adressmasken für Webressourcen

Die Verwendung einer *Adressmaske für eine Webressource* (im Folgenden „Adressmaske“) bietet sich an, wenn eine Zugriffsregel für Webressourcen erstellt wird, für die eine hohe Anzahl ähnlicher Adressen für Webressourcen angegeben werden soll. Eine korrekt formulierte Adressmaske kann eine Vielzahl von Webressourcen ersetzen.

Für das Erstellen einer Adressmaske sind folgende Regeln zu beachten:

1. Das Zeichen `*` ersetzt eine beliebige Abfolge aus null oder mehr Zeichen.

   Beispielsweise wird bei Angabe der Adressmaske `*abc*` die Zugriffsregel für Webressourcen auf alle Adressen angewendet, welche die Zeichenfolge `abc` enthalten. Beispiel: `http://www.example.com/page_0-9abcdef.html`.

2. Mithilfe einer Abfolge des Zeichens `*.` (auch *Domänenmaske* genannt) können Sie alle Domänen einer Adresse auswählen. Die Domänenmaske `*.` ersetzt einen beliebigen Domänennamen, einen Subdomänennamen oder eine leere Zeile.

   Beispiel: Die Maske `*.example.com` steht für die folgenden Adressen:

   - `http://pictures.example.com`. Die Domänenmaske `*.` ersetzt `pictures.`
   - `http://user.pictures.example.com`. Die Domänenmaske `*.` ersetzt `pictures.` und `user.`
   - `http://example.com`. Die Domänenmaske `*.` wird als Leerzeile interpretiert.

3. Die Zeichenfolge `www.` zu Beginn der Adressmaske wird wie `*.` behandelt.

   Beispiel: Die Adressmaske `www.example.com` wird wie `*.example.com` behandelt. Diese Maske schließt die Adressen `www2.example.com` und `www.pictures.example.com` ein.

4. Beginnt eine Adressmaske nicht mit dem Zeichen `*`, entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Präfix `*.`.

5. Endet eine Adressmaske mit einem anderen Zeichen als `/` oder `*`, so entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

   Beispiel: Die Adressmaske `http://www.example.com` schließt Adressen der Form `http://www.example.com/abc` ein, wobei `a`, `b`, `c` für beliebige Zeichen stehen.

6. Endet eine Adressmaske mit dem Zeichen `/`, so entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

7. Die Zeichenfolge `/*` am Ende einer Adressmaske wird wie `/*` oder als leere Zeile behandelt.

8. Eine Untersuchung von Adressen für Webressourcen nach einer Adressmaske erfolgt unter Berücksichtigung des Schemas (http oder https):

   - Enthält eine Adressmaske kein Netzwerkprotokoll, erstreckt sich die Adressmaske auf eine Adresse mit beliebigem Netzwerkprotokoll.

     Beispiel: Die Adressmaske `beispiel.com` umfasst die Adressen `http://beispiel.com` and `https://beispiel.com`.

   - Enthält eine Adressmaske ein Netzwerkprotokoll, erstreckt sich die Adressmaske nur auf Adressen mit dem in der Adressmaske genannten Netzwerkprotokoll.

     Beispiel: Die Adressmaske `http://*.example.com` schließt die Adresse `http://www.example.com` ein, während die Adresse `https://www.example.com` nicht darunter fällt.

9. Eine Adressmaske, die in doppelten Anführungszeichen steht, wird ungeachtet zusätzlicher Substitutionen behandelt. Eine Ausnahme bildet das Zeichen `*`, falls es in der Adressmaske enthalten ist. Für Adressmasken, die

in doppelten Anführungszeichen stehen, werden die Regeln 5 und 7 nicht ausgeführt (s. Beispiele 14 – 18 in folgender Tabelle).

10. Beim Vergleich mit der Adressmaske für eine Webressource bleiben Benutzername und Kennwort, Verbindungsport sowie Groß- und Kleinschreibung unberücksichtigt.

Praktische Beispiele für die Regeln zum Erstellen von Adressmasken

Nr.	Adressmaske	Zu untersuchende Adresse für eine Webressource	Die zu untersuchende Adresse entspricht der Adressmaske	Kommentar
1	*.example.com	http://www.123example.com	Nein	Siehe Regel 1.
2	*.example.com	http://www.123.example.com	Ja	Siehe Regel 2.
3	*example.com	http://www.123example.com	Ja	Siehe Regel 1.
4	*example.com	http://www.123.example.com	Ja	Siehe Regel 1.
5	http://www.*.example.com	http://www.123example.com	Nein	Siehe Regel 1.
6	www.example.com	http://www.example.com	Ja	Siehe Regeln 3, 2 un 1.
7	www.example.com	https://www.example.com	Ja	Siehe Regeln 3, 2 un 1.
8	http://www.*.example.com	http://123.example.com	Ja	Siehe Regeln 3, 4 und 1.
9	www.example.com	http://www.example.com/abc	Ja	Siehe Regeln 3, 5 und 1.
10	example.com	http://www.example.com	Ja	Siehe Regeln 3 und 1
11	http://example.com/	http://example.com/abc	Ja	Siehe Regel 6.
12	http://example.com/*	http://example.com	Ja	Siehe Regel 7.
13	http://example.com	https://example.com	Nein	Siehe Regel 8.
14	„example.com“	http://www.example.com	Nein	Siehe Regel 9.
15	„http://www.example.com“	http://www.example.com/abc	Nein	Siehe Regel 9.
16	„*example.com“	http://www.example.com	Ja	Siehe Regeln 1 und 9
17	„http://www.example.com/*“	http://www.example.com/abc	Ja	Siehe Regeln 1 und 9
18	‚www.example.com“	http://www.example.com; https://www.example.com	Ja	Siehe Regeln 9 und 8
19	www.example.com/abc/123	http://www.example.com/abc	Nein	Eine Adressmaske enthä mehr Informationen als die Adresse eine Webressource.

Migration von Zugriffsregeln für Webressourcen aus Vorgängerversionen des Programms

Beim Programm-Upgrade von der Version Kaspersky Endpoint Security 10 Service Pack 2 für Windows und von älteren Versionen auf die Version Kaspersky Endpoint Security für Windows 11.6.0 erfolgt eine Migration der Zugriffsregeln für Webressourcen, die auf Inhaltskategorien für Webressourcen basieren. Für die Migration gelten die folgenden Regeln:

- Regeln für den Zugriff auf Webressourcen, die auf einer oder mehreren Inhaltskategorien für Webressourcen aus der Liste „Chats und Foren“, „Web-E-Mail“ und „Soziale Netzwerke“ basieren, werden der Webressourcen-Inhaltskategorie „Kommunikation im Internet“ zugeordnet.
- Regeln für den Zugriff auf Webressourcen, die auf einer oder mehreren Inhaltskategorien für Webressourcen aus der Liste „Online-Shops“ und „Zahlungssysteme“ basieren, werden der Webressourcen-Inhaltskategorie „Online-Shops, Banken, Zahlungssysteme“ zugeordnet.
- Regeln für den Zugriff auf Webressourcen, die auf der Inhaltskategorie „Glücksspiel“ basieren, werden der Webressourcen-Inhaltskategorie „Glücksspiel, Lotterien, Wetten“ zugeordnet.
- Regeln für den Zugriff auf Webressourcen, die auf der Inhaltskategorie „Browserspiele“ basieren, werden der Webressourcen-Inhaltskategorie „Computerspiele“ zugeordnet.
- Regeln für den Zugriff auf Webressourcen, die auf Inhaltskategorien basieren, die nicht in den vorstehenden Punkten der Liste enthalten sind, werden unverändert übernommen.

Gerätekontrolle

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die „Gerätekontrolle“ verwaltet den Zugriff von Benutzern auf die Geräte, die installiert oder mit dem Computer verbunden sind (z. B. auf Festplatten, Kamera oder WLAN-Modul). Bei einer Verbindung mit diesen Geräten kann der Computer so vor einer Infektion geschützt werden, und Datenverlust oder Datendiebstahl lassen sich verhindern.

Ebenen für den Zugriff auf Geräte

Die „Gerätekontrolle“ verwaltet den Zugriff auf folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger, CD/DVD-Laufwerke.
  Sie können den Zugriff auf Geräte wie folgt anpassen:
  - Erlauben – ✓.
  - Verbieten – ⊘.

- Von der Schnittstelle abhängig (unter Ausnahme von WLAN) – .
- Block mit Ausnahmen (nur WLAN) – .

- **Schnittstellen**. Mithilfe einer *Verbindungsschnittstelle* können Geräte mit einem Computer verbunden werden (z. B. via USB oder FireWire). Auf diese Weise können Sie beispielsweise für alle Geräte eine Verbindung über USB beschränken.

  Sie können den Zugriff auf Geräte wie folgt anpassen:

  - Erlauben – .
  - Verbieten – .

- **Vertrauenswürdige Geräte**. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

  Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

  - **Geräte nach ID**. Jedes Gerät besitzt eine einmalige ID (engl. Hardware ID – HWID). Die ID finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Beispiel für eine Geräte-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten.
  - **Geräte nach Modell**. Jedes Gerät besitzt eine einmalige Hersteller-ID (engl. Vendor ID – VID) und eine Produkt-ID (engl. Product ID – PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Vorlage für die Eingabe einer VID und PID: `VID_1234&PID_5678`. Es bietet sich an, Geräte mithilfe des Modells hinzuzufügen, wenn Sie in Ihrem Unternehmen Geräte eines bestimmten Modells verwenden. Dadurch können Sie alle Geräte dieses Modells hinzufügen.
  - **Geräte nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs haben, können Sie eine Maske verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.
  - **Geräte nach Modellmaske**. Wenn Sie mehrere Geräte mit ähnlichen VID oder PID verwenden (beispielsweise Geräte desselben Herstellers), können Sie die Geräte mithilfe einer Maske zur Liste der vertrauenswürdigen Geräte hinzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC & PID_ *`.

Die „Gerätekontrolle“ verwendet *Zugriffsregeln*, um den Zugriff von Benutzern auf Geräte zu regulieren. Außerdem kann die „Gerätekontrolle“ Ereignisse über die Verbindung/Trennung von Geräten speichern. Damit Ereignisse gespeichert werden, müssen Sie in der Richtlinie das Senden von Ereignissen anpassen.

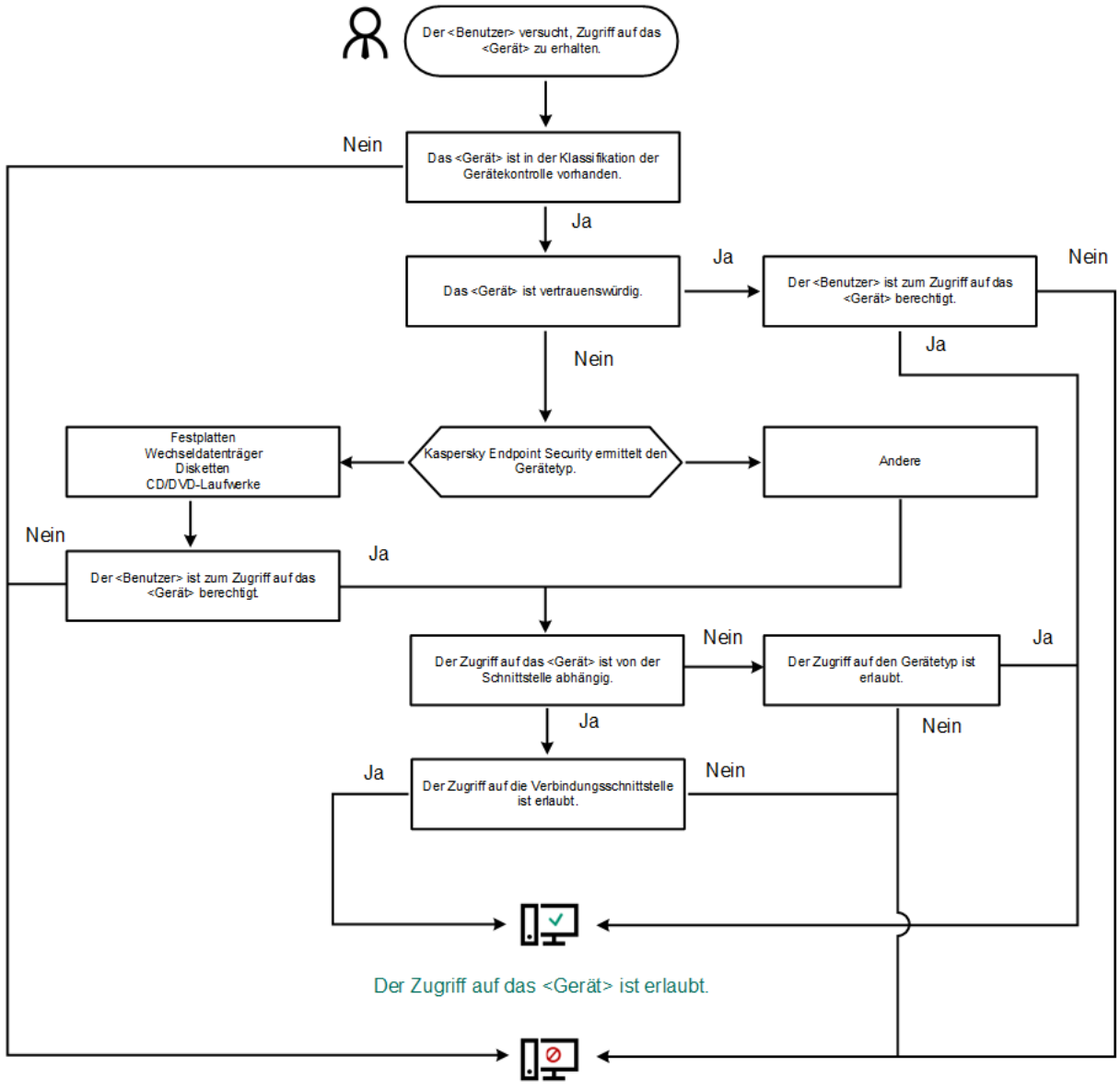
Falls der Zugriff auf das Gerät von der Schnittstelle abhängig ist (Status), werden Ereignisse über die Verbindung/Trennung des Geräts nicht von Kaspersky Endpoint Security gespeichert. Damit das Programm Kaspersky Endpoint Security Ereignisse über die Verbindung/Trennung des Geräts speichert, erlauben Sie den Zugriff auf den entsprechenden Gerätetyp (Status) oder fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

Wird mit dem Computer ein Gerät verbunden, auf das der Zugriff von der „Gerätekontrolle“ verboten ist, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Benachrichtigung an (s. Bild unten).

Benachrichtigung der „Gerätekontrolle"

Algorithmus der „Gerätekontrolle"

Kaspersky Endpoint Security entscheidet über den Zugriff auf ein Gerät, sobald dieses vom Benutzer an den Computer angeschlossen wird (s. folgende Abb.).



Algorithmus der „Gerätekontrolle"

Wenn ein Gerät verbunden ist und der Zugriff erlaubt ist, können Sie die Zugriffsregel ändern und den Zugriff verbieten. Wenn das nächste Mal auf das Gerät zugegriffen wird (Anzeige der Ordnerstruktur, Lesen, Schreiben), blockiert Kaspersky Endpoint Security den Zugriff. Geräte ohne Dateisystem werden erst blockiert, wenn sie zum nächsten Mal mit dem Computer verbunden werden.

Wenn der Benutzer eines Computers, auf dem das Programm Kaspersky Endpoint Security installiert ist, den Zugriff auf ein Gerät angefordert hat, das seiner Meinung nach irrtümlicherweise blockiert wurde, so übermitteln Sie ihm eine Anleitung für die Zugriffsanforderung.

Gerätekontrolle aktivieren und deaktivieren

Die Gerätekontrolle ist standardmäßig aktiviert.

Um die Gerätekontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Verwenden Sie den Schalter **Gerätekontrolle**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Gerätekontrolle aktiviert ist, leitet das Programm Informationen über angeschlossene Geräte an das Kaspersky Security Center weiter. Sie können die Liste der angeschlossenen Geräte im Kaspersky Security Center im Ordner **Hardware** anzeigen.

Über Zugriffsregeln

Zugriffsregeln sind eine Auswahl von Einstellungen, die den Zugriff von Benutzern auf Geräte regulieren, die installiert oder mit dem Computer verbunden sind. Ein Gerät, das nicht zur Klassifikation der „Gerätekontrolle" gehört, kann nicht hinzugefügt werden. Der Zugriff auf diese Geräte ist für alle Benutzer erlaubt.

Regeln für den Zugriff auf Geräte

Die Auswahl der Einstellungen für eine Zugriffsregel ist vom Gerätetyp abhängig (siehe folgende Tabelle).

Einstellungen für eine Zugriffsregel

Geräte	Zugangskontrolle	Zeitplan für den Zugriff auf ein Gerät	Zuweisung von Benutzern / einer Benutzergruppe	Priorität	Erlaubnis zum Lesen/Schreiben
Festplatten	✓	✓	✓	✓	✓
Wechseldatenträger	✓	✓	✓	✓	✓
Drucker	✓	–	–	–	–
Disketten	✓	✓	✓	✓	✓
CD/DVD-Laufwerke	✓	✓	✓	✓	✓

Modems	✓	–	–	–	–
Bandlaufwerke	✓	–	–	–	–
Multifunktionsgeräte	✓	–	–	–	–
Smartcard-Leser	✓	–	–	–	–
Windows CE USB ActiveSync-Geräte	✓	–	–	–	–
Externe Netzwerkadapter	✓	–	–	–	–
Tragbare Geräte (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–
Kameras und Scanner	✓	–	–	–	–

Zugriffsregeln für mobile Geräte

Android- und iOS-Mobilgeräte gelten als tragbare Geräte (MTP). Wenn ein mobiles Gerät mit dem Computer verbunden wird, ermittelt das Betriebssystem den Gerätetyp. Sind auf dem Computer Programme des Typs Android Debug Bridge (ADB), iTunes oder äquivalente Programme installiert, so bestimmt das Betriebssystem die mobilen Geräte als ADB- oder iTunes-Geräte. In den übrigen Fällen kann das Betriebssystem den Typ eines mobilen Gerätes als tragbares Gerät (MTP) für die Dateiübertragung, als PTP-Geräte (Kamera) für die Bildübertragung oder als anderes Gerät bestimmen. Der Gerätetyp ist vom Modell des mobilen Gerätes abhängig.

Für den Zugriff auf ADB- oder iTunes-Geräte gelten die folgenden Besonderheiten:

- Es ist nicht möglich, einen Zeitplan für den Zugriff auf ein Gerät einzurichten. Das bedeutet, wenn der Zugriff auf Geräte durch Regeln beschränkt ist (Status), sind ADB- und iTunes-Geräte immer verfügbar.
- Es ist nicht möglich, den Zugriff auf ein Gerät für bestimmte Benutzer oder die Zugriffsrechte (Lesen / Schreiben) anzupassen. Das bedeutet, wenn der Zugriff auf Geräte durch Regeln beschränkt ist (Status), sind ADB- und iTunes-Geräte für alle Benutzer mit beliebigen Rechten verfügbar.
- Es ist nicht möglich, den Zugriff auf vertrauenswürdige ADB- und iTunes-Geräte für bestimmte Benutzer anzupassen. Wenn ein Gerät vertrauenswürdig ist, sind ADB- und iTunes-Geräte für alle Benutzer verfügbar.
- Wenn Sie ADB- oder iTunes-Programme installiert haben, nachdem ein Gerät mit dem Computer verbunden wurde, kann es sein, dass die einmalige Geräte-ID zurückgesetzt wird. Das bedeutet, dass Kaspersky Endpoint Security dieses Gerät als neu erkennt. Wenn das Gerät vertrauenswürdig ist, fügen Sie es erneut zur Liste der vertrauenswürdigen Geräte hinzu.

Regeln für den Zugriff auf Geräte erlauben standardmäßig allen Benutzern jederzeit den vollständigen Zugriff auf Geräte, vorausgesetzt, der Zugriff auf Schnittstellen für die entsprechenden Gerätetypen ist erlaubt (Status).

Regeln für den Zugriff auf WLAN-Netzwerke

Eine Regel für den Zugriff auf WLAN-Netzwerke legt die Erlaubnis (Status ✓) oder das Verbot (Status ⊘) für die Verwendung von WLAN-Netzwerken fest. Sie können ein *vertrauenswürdiges WLAN-Netzwerk* (Status) zu einer Regel hinzufügen. Verwendung eines vertrauenswürdigen WLAN-Netzwerks ohne Beschränkungen. Eine Regel für den Zugriff auf ein WLAN-Netzwerk erlaubt standardmäßig den Zugriff auf ein beliebiges WLAN-Netzwerk.

Regeln für den Zugriff auf Verbindungsschnittstellen

Regeln für den Zugriff auf Schnittstellen legen nur die Erlaubnis (Status ✓) oder das Verbot (Status ⊘) für die Verbindung mit Geräten fest. Für alle Schnittstellen aus der Klassifikation der Komponente „Gerätekontrolle“ sind standardmäßige Regeln erstellt, die den Zugriff auf die Schnittstellen erlauben.

Zugriffsregel für ein Gerät ändern

Eine *Gerätezugriffsregel* ist eine Gruppe von Einstellungen, mit deren Hilfe Benutzer auf installierte oder an den Computer angeschlossene Geräte zugreifen können. Zu diesen Einstellungen gehören der Zugriff auf ein bestimmtes Gerät, ein Zugriffszeitplan sowie Lese- oder Schreibberechtigungen.

Gehen Sie folgendermaßen vor, um eine Regel für den Zugriff auf ein Gerät zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Zugriff anpassen** auf die Schaltfläche **Geräte und WLAN-Netzwerke**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.
4. Wählen Sie im Block **Zugriff auf Speichergeräte** die Zugriffsregel aus, die Sie bearbeiten möchten. Der Block enthält Geräte, die über ein Dateisystem verfügen, für das Sie zusätzliche Zugriffseinstellungen konfigurieren können. Standardmäßig erlaubt eine Zugriffsregel für Geräte allen Benutzern jederzeit den vollständigen Zugriff auf einen Gerätetyp.

   a. Wählen Sie im Block **Zugriff** die entsprechende Gerätezugriffsoption:

   - **Erlauben**.
   - **Blockieren**
   - **Von Verbindungsschnittstelle abhängig**

     Um den Zugriff auf ein Gerät zu blockieren oder zuzulassen, konfigurieren Sie den Zugriff auf die Schnittstelle.
   - **Durch Regeln einschränken**

     Mit dieser Option können Sie Benutzerrechte, Berechtigungen und einen Zeitplan für den Gerätezugriff konfigurieren.

   b. Klicken Sie im Block **Benutzerrechte** auf die Schaltfläche **Hinzufügen**.

   Dies öffnet ein Fenster zum Hinzufügen einer neuen Gerätezugriffsregel.

   c. Weisen Sie der *Regel* eine Priorität zu. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben) und Priorität.

Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Endpoint Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

Beispielsweise können Sie der Gruppe "Jeder" schreibgeschützte Leseberechtigungen und der Gruppe "Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

d. Wählen Sie den Status **Aktiviert** für die Gerätezugriffsregel.

e. Konfigurieren Sie die Gerätezugriffsberechtigungen der Benutzer: Lesen und/oder Schreiben.

f. Wählen Sie die Benutzer oder Benutzergruppen aus, auf die Sie die Gerätezugriffsregel anwenden möchten.

g. Konfigurieren Sie einen Gerätezugriffsplan für Benutzer.

h. Klicken Sie auf **Hinzufügen**.

5. Wählen Sie im Block **Zugriff auf externe Geräte** die Regel aus und konfigurieren Sie den Zugriff: **Zulassen**, **Verweigern** oder **Abhängig von der Verbindungsschnittstelle**. Konfigurieren Sie erforderlichenfalls den Zugriff auf die Verbindungsschnittstelle.

6. Klicken Sie im Block **Zugriff auf WLAN-Netzwerke** auf den Link **WLAN** und konfigurieren Sie den Zugriff: **Erlauben**, **Blockieren** oder **Verbieten mit Ausnahmen**. Fügen Sie ggf. WLAN-Netzwerke zur vertrauenswürdigen Liste hinzu.

7. Speichern Sie die vorgenommenen Änderungen.

Zugriffsregel für eine Verbindungsschnittstelle ändern

Gehen Sie folgendermaßen vor, um eine Zugriffsregel für eine Schnittstelle zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.

3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Schnittstellen**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.

4. Wählen Sie eine Zugriffsregel, die geändert werden soll.

5. Wählen Sie in der Spalte **Zugriff**, ob Sie den Zugriff auf die Schnittstelle erlauben oder verweigern möchten: **Zulassen** oder **Verweigern**.

6. Speichern Sie die vorgenommenen Änderungen.

WLAN-Netzwerk zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzufügen

Sie können den Benutzern erlauben, sich mit WLAN-Netzwerken zu verbinden, die Sie für sicher halten, zum Beispiel mit dem WLAN-Netzwerk Ihres Unternehmens. Dazu muss dieses Netzwerk zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzugefügt werden. Die Gerätekontrolle blockiert den Zugriff auf alle WLAN-Netzwerke, außer jenen, welche auf der Liste der vertrauenswürdigen WLAN-Netzwerke stehen.

Um ein WLAN-Netzwerk zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.
4. Klicken Sie im Block **Zugriff auf WLAN-Netzwerke** auf die **WLAN**-Verknüpfung.

   Das geöffnete Fenster zeigt die Regeln für den WLAN-Zugriff.
5. Wählen Sie in der Spalte **Zugriff** die Option **Mit Ausnahmen blockieren**.
6. Klicken Sie auf die Schaltfläche **Hinzufügen** im Block **Vertrauenswürdiges WLAN-Netzwerk**.
7. Gehen Sie im geöffneten Fenster wie folgt vor:

   a. Geben Sie im Feld **Netzwerkname** den Namen des WLAN-Netzwerks an, das Sie zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzufügen möchten.

   b. Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** den Authentifizierungstyp, der bei einer Verbindung mit dem vertrauenswürdigen WLAN-Netzwerk verwendet werden soll.

   c. Wählen Sie in der Dropdown-Liste **Verschlüsselungstyp** den Verschlüsselungstyp, mit dem der Datenverkehr des vertrauenswürdigen WLAN-Netzwerks geschützt werden soll.

   d. Im Feld **Kommentar** können Sie beliebige Informationen über das hinzuzufügende WLAN-Netzwerk angeben.

   Ein WLAN-Netzwerk wird als vertrauenswürdig betrachtet, wenn seine Einstellungen mit den in der Regel angegebenen Einstellungen übereinstimmen.
8. Speichern Sie die vorgenommenen Änderungen.

Überwachung der Nutzung von Wechseldatenträgern

So aktivieren Sie die Überwachung der Nutzung von Wechseldatenträgern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.
4. Wählen Sie im Block **Zugriff auf Speichergeräte** die Option **Wechseldatenträger**.
5. Klicken Sie auf **Ereignisprotokollierung**.
6. Wählen Sie im geöffneten Fenster die Registerkarte **Protokollierung**.
7. Aktivieren Sie den Schalter **Ereignisprotokollierung**.
8. Markieren Sie im Block **Vorgänge mit Dateien** die Operationen, die Sie überwachen möchten: **Schreiben**, **Löschen**.
9. Wählen Sie im Block **Filter nach Dateiformaten** die Formate von Dateien aus, deren zugehörige Operationen von der Gerätekontrolle protokolliert werden sollen.
10. Wählen Sie die Benutzer oder Benutzergruppen aus, deren Verwendung von Wechsellaufwerken Sie überwachen möchten.
11. Speichern Sie die vorgenommenen Änderungen.

Wenn daher Benutzer Dateien speichern, die sich auf Wechseldatenträgern befinden, oder Dateien von Wechseldatenträgern löschen, so speichert Kaspersky Endpoint Security im Ereignisprotokoll Informationen über den ausgeführten Vorgang und sendet ein Ereignis an das Kaspersky Security Center. Ereignisse, die mit Dateien auf Wechseldatenträgern zusammenhängen, können Sie in der Verwaltungskonsole für Kaspersky Security Center im Arbeitsbereich für den Knoten **Administrationsserver** auf der Registerkarte **Ereignisse** einsehen. Damit Ereignisse im lokalen Ereignisprotokoll von Kaspersky Endpoint Security angezeigt werden, muss das Kontrollkästchen **Ein Dateivorgang wurde ausgeführt** in den Benachrichtigungseinstellungen für die Komponente „Gerätekontrolle“ aktiviert werden.

Ändern der Cache-Dauer

Die Komponente „Gerätekontrolle“ registriert Ereignisse im Zusammenhang mit überwachten Geräten, wie das Anschließen und Trennen eines Geräts, das Lesen einer Datei von einem Gerät, das Schreiben einer Datei auf ein Gerät und andere Ereignisse. Gerätekontrolle erlaubt oder blockiert dann die Aktion entsprechend den Einstellungen von Kaspersky Endpoint Security.

Die Gerätekontrolle speichert Informationen über Ereignisse für einen bestimmten Zeitraum, den sogenannten *Caching-Zeitraum*. Wenn Informationen über ein Ereignis zwischengespeichert werden und dieses Ereignis wiederholt wird, ist es nicht notwendig, Kaspersky Endpoint Security darüber zu informieren oder eine weitere Aufforderung zur Gewährung des Zugriffs auf die entsprechende Aktion, wie z. B. das Anschließen eines Geräts, anzuzeigen. Dadurch wird die Arbeit mit einem Gerät komfortabler.

Ein Ereignis wird als doppeltes Ereignis betrachtet, wenn alle folgenden Ereigniseinstellungen mit dem Datensatz im Cache übereinstimmen:

- Geräte-ID

- SID des Benutzerkontos, auf das zugegriffen werden soll
- Gerätekategorie
- Mit dem Gerät ergriffene Maßnahmen
- Entscheidung über die Erlaubnis für das Programm für diese Aktion: erlaubt oder verweigert
- Pfad zum Prozess, der zur Durchführung der Aktion verwendet wurde
- Datei, auf die zugegriffen wird

Deaktivieren Sie Selbstschutz für Kaspersky Endpoint Security, bevor Sie den Cache-Zeitraum ändern. Aktivieren Sie den Selbstschutz, nachdem Sie den Cache-Zeitraum geändert haben.

So ändern Sie den Cache-Zeitraum:

1. Öffnen Sie den Registrierungseditor auf dem Computer.
2. Gehen Sie im Registrierungseditor zum folgenden Abschnitt:
   - Für 64-Bit-Betriebssysteme:
     [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
   - Für 32-Bit-Betriebssysteme:
     [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]
3. Öffnen Sie DeviceControlEventsCachePeriod zur Bearbeitung.
4. Definieren Sie die Anzahl der Minuten, die die Gerätesteuerung Informationen über ein Ereignis speichern muss, bevor diese Informationen gelöscht werden.

Aktionen für vertrauenswürdige Geräte

Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Sie können entweder einem einzelnen Benutzer, einer Benutzergruppe oder allen Benutzern des Unternehmens den Zugriff auf vertrauenswürdige Geräte gewähren.

Wenn in Ihrem Unternehmen beispielsweise die Verwendung von Wechseldatenträgern verboten ist, aber die Administratoren für ihre Arbeit Wechseldatenträger verwenden, können Sie die Verwendung von Wechseldatenträgern nur für die Gruppe der Administratoren erlauben. Dazu müssen Wechseldatenträger zur Liste der vertrauenswürdigen Geräte hinzugefügt werden und die Zugriffsrechte für Benutzer angepasst werden.

In Kaspersky Endpoint Security kann ein Gerät wie folgt zur Liste der vertrauenswürdigen Geräte hinzugefügt werden:

- Wenn die Lösung Kaspersky Security Center in Ihrem Unternehmen nicht bereitsteht, können Sie ein Gerät mit dem Computer verbinden und es in den Programmeinstellungen zur Liste der vertrauenswürdigen Geräte hinzufügen. Um eine Liste der vertrauenswürdigen Geräte an alle Computer des Unternehmens zu verteilen, können Sie in der Richtlinie die Funktion zur Zusammenfassung der Listen mit den vertrauenswürdigen Geräten aktivieren und den Export-/Importvorgang verwenden.

- Wenn die Lösung Kaspersky Security Center in Ihrem Unternehmen bereitgestellt wurde, können Sie per Fernzugriff alle verbundenen Geräte ermitteln und in der Richtlinie eine Liste der vertrauenswürdigen Geräte erstellen. Die Liste der vertrauenswürdigen Geräte ist auf allen Geräten verfügbar, auf welche die Richtlinie an angewendet wird.

Kaspersky Endpoint Security hat die folgenden Einschränkungen bei der Arbeit mit vertrauenswürdigen Geräten:

- Das Kaspersky Endpoint Security Verwaltungs-Plug-In der Versionen 11.0.0-11.2.0 kann nicht mit einer Liste vertrauenswürdiger Geräte arbeiten, die mit Kaspersky Endpoint Security Version 11.3.0 und 11.4.0 erstellt wurde. Um mit einer Liste von vertrauenswürdigen Geräten aus diesen Versionen arbeiten zu können, muss das Verwaltungs-Plug-in auf Version 11.3.0 bzw. 11.4.0 aktualisiert werden.

- Das Kaspersky Endpoint Security Verwaltungs-Plug-In Version 11.3.0 und 11.4.0 kann nicht mit einer Liste vertrauenswürdiger Geräte arbeiten, die in Kaspersky Endpoint Security Version 11.2.0 oder früher erstellt wurde. Damit diese Versionen mit einer Liste von vertrauenswürdigen Geräten funktionieren, muss das Programm auf Version 11.3.0 bzw. 11.4.0 aktualisiert werden. Eine Anfrage mit einer Beschreibung Ihrer Situation können Sie auch über Kaspersky CompanyAccount an den Technischen Support senden.

- Um eine Liste der vertrauenswürdigen Geräte von Kaspersky Endpoint Security Version 11.2.0 auf Version 11.3.0 zu migrieren, senden Sie über Kaspersky CompanyAccount eine Anfrage mit einer Beschreibung Ihrer Situation an den Technischen Support.

Gerät von der Programmoberfläche aus zur Liste der vertrauenswürdigen Geräte hinzufügen

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe Jeder).

Gehen Sie folgendermaßen vor, um ein Gerät von der Programmoberfläche aus zur Liste der vertrauenswürdigen Geräte hinzuzufügen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.
4. Klicken Sie auf **Auswählen**.

   Dadurch wird die Liste der angeschlossenen Geräte geöffnet. Die Liste der Geräte hängt von dem Wert ab, der in der Dropdown-Liste **Angeschlossene Geräte anzeigen** ausgewählt ist.
5. Wählen Sie in der Geräteliste das Gerät aus, das Sie zur Liste der vertrauenswürdigen Geräte hinzufügen möchten.
6. Im Feld **Kommentar** können Sie alle relevanten Informationen über das vertrauenswürdige Gerät angeben.
7. Wählen Sie die Benutzer oder Benutzergruppen aus, denen Sie den Zugriff auf vertrauenswürdige Geräte erlauben möchten.
8. Speichern Sie die vorgenommenen Änderungen.

Gerät zur Liste der vertrauenswürdigen Geräte aus Kaspersky Security Center hinzufügen

Kaspersky Security Center erhält Informationen über die Geräte, wenn auf den Computern das Programm Kaspersky Endpoint Security installiert ist und die Gerätekontrolle aktiviert ist. Ein Gerät, über das in Kaspersky Security Center keine Informationen vorliegen, kann nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

Mithilfe der folgenden Daten können Sie ein Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen:

- **Geräte nach ID**. Jedes Gerät besitzt eine einmalige ID (engl. Hardware ID – HWID). Die ID finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Beispiel für eine Geräte-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten.

- **Geräte nach Modell**. Jedes Gerät besitzt eine einmalige Hersteller-ID (engl. Vendor ID – VID) und eine Produkt-ID (engl. Product ID – PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Vorlage für die Eingabe einer VID und PID: `VID_1234&PID_5678`. Es bietet sich an, Geräte mithilfe des Modells hinzuzufügen, wenn Sie in Ihrem Unternehmen Geräte eines bestimmten Modells verwenden. Dadurch können Sie alle Geräte dieses Modells hinzufügen.

- **Geräte nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs haben, können Sie eine Maske verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.

- **Geräte nach Modellmaske**. Wenn Sie mehrere Geräte mit ähnlichen VID oder PID verwenden (beispielsweise Geräte desselben Herstellers), können Sie die Geräte mithilfe einer Maske zur Liste der vertrauenswürdigen Geräte hinzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC & PID_ *`.

Um ein Gerät zur Liste der vertrauenswürdigen Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

5. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.

6. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.

7. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine gemeinsame Liste der vertrauenswürdigen Geräte für alle Computer des Unternehmens erstellen möchten.

Die Listen mit vertrauenswürdigen Geräten der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Geräte der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Geräte der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.

8. Klicken Sie auf **Hinzufügen** und wählen Sie die Methode aus, mit der das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt werden soll.

9. Um die Geräte zu filtern, wählen Sie in der Dropdown-Liste **Gerätetyp** einen Gerätetyp aus (z. B. **Wechseldatenträger**).

10. Geben Sie im Feld **Name / Modell** die Geräte-ID, das Modell (VID und PID) oder eine Maske ein. Die Eingabe ist von der ausgewählten Methode für das Hinzufügen abhängig.

    Das Hinzufügen von Geräten nach Modellmaske (VID und PID) funktioniert folgendermaßen: Wenn Sie eine Modellmaske eingeben, die mit keinem Modell übereinstimmt, prüft Kaspersky Endpoint Security, ob die Geräte-ID (HWID) mit der Maske übereinstimmt. Kaspersky Endpoint Security überprüft nur den Teil der Geräte-ID, der den Hersteller und den Gerätetyp angibt (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Wenn die Modellmaske diesem Teil der Geräte-ID entspricht, werden auf dem Computer zur Liste der vertrauenswürdigen Geräte jene Geräte hinzugefügt, die der Maske entsprechen. Wenn Sie in Kaspersky Security Center auf **Aktualisieren** klicken, wird in diesem Fall eine leere Geräteliste angezeigt. Damit die Geräteliste korrekt angezeigt wird, können Sie die Geräte mithilfe einer Maske für die Geräte-ID hinzufügen.

11. Um die Geräte zu filtern, geben Sie im Feld **Computer** den Namen des Computers oder eine Namensmaske des Computers ein, mit dem das Gerät verbunden ist.

    Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` steht als Platzhalter für ein beliebiges Einzelzeichen.

12. Klicken Sie auf **Aktualisieren**.

    In der Tabelle wird eine Liste der Geräte angezeigt, die den angegebenen Filterbedingungen entsprechen.

13. Aktivieren Sie die Kontrollkästchen für jene Geräte, die zur Liste der vertrauenswürdigen Geräte hinzugefügt werden sollen.

14. Geben Sie im Feld **Kommentar** an, weshalb das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt wird.

15. Klicken Sie rechts vom Feld **Für Benutzer und/oder Benutzergruppen erlauben** auf **Auswählen**.

16. Wählen Sie einen Benutzer oder eine Gruppe in Active Directory aus und bestätigen Sie Ihre Auswahl.

    Für die Gruppe „Alle“ ist der Zugriff auf vertrauenswürdige Geräte standardmäßig erlaubt.

17. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Gerät angeschlossen wird, überprüft Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte für den autorisierten Benutzer. Wenn das Gerät vertrauenswürdig ist, erlaubt Kaspersky Endpoint Security den Zugriff auf das Gerät mit allen Rechten, sogar wenn der Zugriff auf diesen Gerätetyp oder auf diese Schnittstelle verboten ist. Wenn das Gerät nicht vertrauenswürdig ist und der Zugriff verboten ist, können Sie Zugriff auf das blockierte Gerät anfordern.

Liste mit vertrauenswürdigen Geräten exportieren und importieren

Um die Liste der vertrauenswürdigen Geräte an alle Computer des Unternehmens zu verteilen, können Sie die Liste exportieren bzw. importieren.

Um beispielsweise eine Liste der vertrauenswürdigen Wechseldatenträger zu verteilen, gehen Sie wie folgt vor:

1. Verbinden Sie die Wechseldatenträger nacheinander mit dem Computer.
2. Fügen Sie die Wechseldatenträger in den Einstellungen von Kaspersky Endpoint Security zur Liste der vertrauenswürdigen Wechseldatenträger hinzu. Passen Sie bei Bedarf die Zugriffsrechte der Benutzer an. Sie können beispielsweise den Zugriff auf Wechseldatenträger nur den Administratoren erlauben.
3. Exportieren Sie in den Einstellungen von Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte (s. Anleitung unten).
4. Verteilen Sie die Datei mit der Liste der vertrauenswürdigen Geräte an die übrigen Computer des Unternehmens. Sie können die Datei beispielsweise in einem gemeinsamen Ordner ablegen.
5. Importieren Sie in den Einstellungen von Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte auf die übrigen Computern des Unternehmens (s. Anleitung unten).

Um die Liste mit vertrauenswürdigen Geräten zu importieren oder exportieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.
4. Um die Liste der vertrauenswürdigen Geräte zu exportieren, gehen Sie wie folgt vor:

   a. Wählen Sie die vertrauenswürdigen Geräte aus, die Sie exportieren möchten.

   b. Klicken Sie auf **Export**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der vertrauenswürdigen Geräte exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Klicken Sie auf **Speichern**.

   Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Geräte in die XLM-Datei.
5. Um die Liste der vertrauenswürdigen Geräte zu importieren, gehen Sie wie folgt vor:

   a. Wählen Sie in der Dropdown-Liste **Import** die entsprechende Aktion aus: **Importieren und hinzufügen** oder **Importieren und ersetzen**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Geräte importieren möchten.

   c. Klicken Sie auf **Öffnen**.

   Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Geräten gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Gerät angeschlossen wird, überprüft Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte für den autorisierten Benutzer. Wenn das Gerät vertrauenswürdig ist, erlaubt Kaspersky Endpoint Security den Zugriff auf das Gerät mit allen Rechten, sogar wenn der Zugriff auf diesen Gerätetyp oder auf diese Schnittstelle verboten ist.

Freigabe eines blockierten Geräts

Es kann vorkommen, dass Sie beim Anpassen der „Gerätekontrolle“ versehentlich den Zugriff auf ein erforderliches Gerät verbieten.

Falls in Ihrem Unternehmen die Lösung Kaspersky Security Center nicht verteilt wurde, können Sie das Gerät in den Einstellungen für Kaspersky Endpoint Security freigeben. Beispielsweise können Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen oder die Gerätekontrolle vorübergehend deaktivieren.

Falls in Ihrem Unternehmen die Lösung Kaspersky Security Center verteilt wurde und auf die Computer eine Richtlinie angewendet wurde, können Sie das Gerät in der Verwaltungskonsole freigeben.

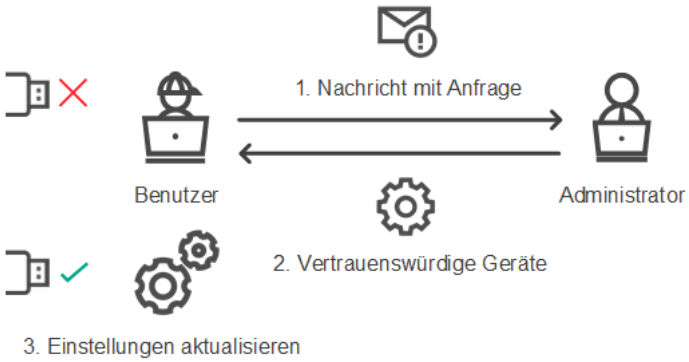
Online-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Online-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. Der Computer muss die Möglichkeit haben, eine Verbindung zum Administrationsserver herzustellen.

Die Freigabe im Online-Modus umfasst die folgenden Schritte:

1. Der Benutzer sendet an den Administrator eine Nachricht mit einer Freigabeanfrage.
2. Der Administrator fügt das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

   Ein vertrauenswürdiges Gerät können Sie in der Richtlinie für die Administrationsgruppe hinzufügen oder in den lokalen Programmeinstellungen für einen bestimmten Computer.
3. Der Administrator aktualisiert die Einstellungen für Kaspersky Endpoint Security auf dem Benutzercomputer.



Schema für die Freigabe eines Gerätes im Online-Modus

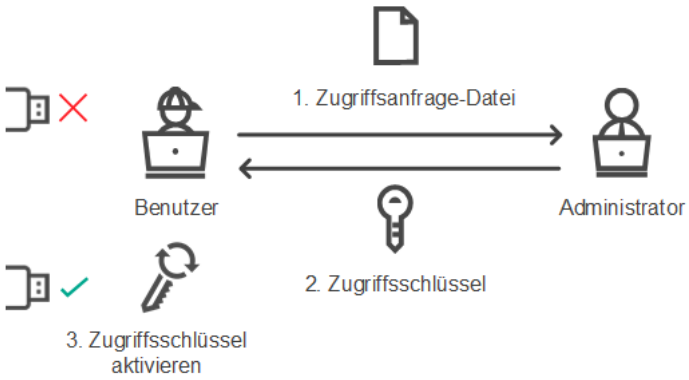
Offline-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Offline-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. In den Einstellungen der Richtlinie im Abschnitt **Gerätekontrolle** muss das Kontrollkästchen **Anfrage auf temporären Zugriff erlauben** aktiviert sein.

Falls ein blockiertes Gerät vorübergehend freigegeben werden soll, das Gerät aber nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden kann, können Sie das Gerät im Offline-Modus freigeben. Auf diese Weise können Sie ein blockiertes Gerät freigeben, falls Ihr Computer keinen Netzwerkzugang hat oder falls sich der Computer außerhalb des Unternehmensnetzwerks befindet.

Die Freigabe im Offline-Modus umfasst die folgenden Schritte:

1. Der Benutzer erstellt eine Zugriffsanfrage-Datei und sendet sie an den Administrator.
2. Der Administrator erstellt mithilfe der Zugriffsanfrage-Datei einen Zugriffsschlüssel und sendet ihn an den Benutzer.
3. Der Benutzer aktiviert den Zugriffsschlüssel.



Schema für die Freigabe eines Gerätes im Offline-Modus

Online-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Online-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. Der Computer muss die Möglichkeit haben, eine Verbindung zum Administrationsserver herzustellen.

Um als Benutzer den Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

1. Verbinden Sie das Gerät mit dem Computer.

   Kaspersky Endpoint Security zeigt eine Benachrichtigung darüber an, dass der Zugriff auf das Gerät blockiert wurde (siehe folgende Abb.).

2. Klicken Sie auf den Link **Zugriff erfragen**.

   Das Fenster **Nachricht an den Administrator** wird geöffnet. Die Nachricht enthält Informationen über das blockierte Gerät.

3. Klicken Sie auf **Senden**.

Der Administrator erhält z. B. per E-Mail eine Nachricht mit einer Freigabeanfrage. Details über die Verarbeitung von Benutzeranfragen finden Sie in der *Hilfe zu Kaspersky Security Center*. Nachdem das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt und die Einstellungen für Kaspersky Endpoint Security auf dem Computer aktualisiert wurden, erhält der Benutzer Zugriff auf das Gerät.

Benachrichtigung der „Gerätekontrolle"

Offline-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Offline-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. In den Einstellungen der Richtlinie im Abschnitt **Gerätekontrolle** muss das Kontrollkästchen **Anfrage auf temporären Zugriff erlauben** aktiviert sein.

Um als Benutzer den Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

1. Verbinden Sie das Gerät mit dem Computer.

   Kaspersky Endpoint Security zeigt eine Benachrichtigung darüber an, dass der Zugriff auf das Gerät blockiert wurde (siehe folgende Abb.).

2. Klicken Sie auf den Link **Temporären Zugriff anfordern**.

   Das Fenster **Zugriff auf ein Gerät erfragen** mit einer Liste der verbundenen Geräte wird geöffnet.

3. Wählen Sie in der Liste der angeschlossenen Geräte das Gerät aus, auf das Sie zugreifen möchten.

4. Klicken Sie auf **Zugriffsanfrage-Datei erstellen**.

5. Geben Sie im Feld **Dauer des Zugriffs auf das Gerät** den Zeitraum an, für den Sie Zugriff auf das Gerät erhalten möchten.

6. Speichern Sie die Datei auf dem Computer.

   Dadurch wird eine Zugriffsanfrage-Datei mit der Erweiterung *.akey auf den Computer geladen. Senden Sie die Zugriffsanfrage-Datei für das Gerät auf beliebige Weise an den Administrator des lokalen Unternehmensnetzwerks.

Benachrichtigung der „Gerätekontrolle"

Um als Administrator einen Zugriffsschlüssel für ein blockiertes Gerät zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie in der Liste der Client-Computer den Computer aus, dessen Benutzer temporären Zugriff auf ein gesperrtes Gerät erhalten soll.
5. Wählen Sie im Kontextmenü des Computers den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Gerätekontrolle** aus.
7. Klicken Sie auf **Durchsuchen** und öffnen Sie die Zugriffsanfrage-Datei, die Sie vom Benutzer erhalten haben.

   Es werden Informationen über das blockierte Gerät angezeigt, auf das der Benutzer den Zugriff erfragt hat.
8. Ändern Sie erforderlichenfalls den Wert der Einstellung **Dauer des Zugriffs auf das Gerät**.

   Für die Einstellung **Dauer des Zugriffs auf das Gerät** ist standardmäßig der Wert festgelegt, der vom Benutzer bei der Erstellung der Zugriffsanfrage-Datei angegeben wurde.
9. Geben Sie einen Wert für **Aktivierungszeitraum** an.

   Diese Einstellung enthält den Zeitraum, während dem der Benutzer mithilfe des Zugriffsschlüssels den Zugriff auf das blockierte Gerät aktivieren kann.
10. Speichern Sie die Schlüsseldatei auf dem Computer.

Dadurch wird der Zugriffsschlüssel für das blockierte Gerät auf den Computer geladen. Die Zugriffsschlüsseldatei hat die Erweiterung *.acode. Senden Sie den Zugriffsschlüssel für das blockierte Gerät auf beliebige Weise an den Benutzer.

Um als Benutzer den Zugriffsschlüssel zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Zugriffsanforderung** auf die Schaltfläche **Zugriff auf ein Gerät erfragen**.

4. Klicken Sie im geöffneten Fenster auf die Schaltfläche **Zugriffsschlüssel aktivieren**.

5. Wählen Sie im folgenden Fenster die Datei mit dem Zugriffsschlüssel für das Gerät aus, die Sie vom Administrator des lokalen Unternehmensnetzwerks erhalten haben. Klicken Sie auf **Öffnen**.

   Ein Fenster mit Informationen über die Freigabe wird geöffnet.

6. Klicken Sie auf **OK**.

Dadurch erhält der Benutzer für den vom Administrator festgelegten Zeitraum Zugriff auf das Gerät. Der Benutzer erhält einen kompletten Berechtigungssatz für den Zugriff auf das Gerät (Schreiben und Lesen). Wenn der Zugriffsschlüssel abläuft, wird der Zugriff auf das Gerät blockiert. Falls der Benutzer permanenten Zugriff auf das Gerät benötigt, fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

Meldungsvorlagen für die Gerätekontrolle ändern

Versucht ein Benutzer, auf ein blockiertes Gerät zuzugreifen, so meldet Kaspersky Endpoint Security die Sperrung des Geräts oder das Verbot für einen Vorgang mit dem Geräteinhalt. Ist der Benutzer der Meinung, die Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt sei irrtümlich erfolgt, so kann der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden. Dafür ist im Text der Sperrmeldung ein Link vorgesehen.

Für die Meldung über die Sperrung eines Geräts oder über das Verbot eines Vorgangs mit dem Geräteinhalt, sowie für die Nachricht an den Administrator sind Vorlagen vorgesehen. Die Meldungsvorlagen können geändert werden.

Um die Meldungsvorlagen für die Gerätekontrolle zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Gerätekontrolle**.

3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Gerätekontrolle:

   - **Nachricht zum Blockieren**. Vorlage der Nachricht, die erscheint, wenn der Benutzer auf ein blockiertes Gerät zugreift. Diese Nachricht erscheint auch, wenn der Benutzer versucht, einen Vorgang mit dem Geräteinhalt auszuführen, zu dem dieser Benutzer nicht berechtigt ist.

   - **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn die Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt nach Meinung des Benutzers irrtümlicherweise erfolgt.

4. Speichern Sie die vorgenommenen Änderungen.

Anti-Bridging

Anti-Bridging verhindert die Erstellung von Netzwerkbrücken und verhindert zu diesem Zweck, dass gleichzeitig mehrere Netzwerkverbindungen für den Computer hergestellt werden. Dadurch kann das Unternehmensnetzwerk vor Angriffen über ungeschützte und nicht autorisierte Netzwerke geschützt werden.

Anti-Bridging reguliert die Herstellung von Netzwerkverbindungen und verwendet dazu *Verbindungsregeln*.

Für die folgenden vordefinierten Gerätetypen sind bereits Verbindungsregeln vorhanden:

- Netzwerkadapter
- WLAN-Adapter
- Modems

Wenn eine Verbindungsregel aktiviert ist, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Wird eine neue Verbindung hergestellt, so wird die aktive Verbindung blockiert, falls für beide Verbindungen der in der Regel angegebene Gerätetyp verwendet wird.
- Verbindungen werden blockiert, wenn Sie mithilfe von Gerätetypen, für die Regeln mit einer niedrigeren Priorität verwendet werden, hergestellt wurden oder hergestellt werden sollen.

Anti-Bridging aktivieren

Die Funktion Anti-Bridging ist standardmäßig deaktiviert.

So aktivieren Sie Anti-Bridging:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Anti-Bridging**.
4. Verwenden Sie den Schalter **Anti-Bridging aktivieren**, um diese Funktion zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

Nachdem die Funktion Anti-Bridging aktiviert wurde, blockiert Kaspersky Endpoint Security die bereits bestehenden Verbindungen gemäß der Verbindungsregeln.

Status einer Verbindungsregel ändern

Im den Status einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Anti-Bridging**.
4. Wählen Sie im Block **Regeln für Geräte** die Regel aus, deren Status Sie ändern möchten.
5. Verwenden Sie die Schalter in der Spalte **Kontrolle**, um die Regel zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

Priorität einer Verbindungsregel ändern

Im die Priorität einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Gerätekontrolle**.
3. Klicken Sie im Block **Einstellungen** auf die Schaltfläche **Anti-Bridging**.
4. Wählen Sie im Block **Regeln für Geräte** die Regel aus, deren Priorität Sie ändern möchten.
5. Verwenden Sie die Schaltflächen **Aufwärts** / **Abwärts**, um die Priorität der Verbindungsregel festzulegen.

   Je höher die Position einer Regel in der Tabelle ist, desto höher ist ihre Priorität. Die Funktion Anti-Bridging blockiert alle Verbindungen, unter Ausnahme der Verbindung, die mithilfe des Gerätetyps hergestellt wurde, für welchen die Regel mit der höchsten Priorität verwendet wird.
6. Speichern Sie die vorgenommenen Änderungen.

Adaptive Kontrolle von Anomalien

Diese Komponente ist nur für Kaspersky Endpoint Security for Business Advanced und Kaspersky Total Security for Business verfügbar. Ausführliche Informationen über Kaspersky Endpoint Security for Business finden Sie auf der *Kaspersky-Website*.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Adaptive Kontrolle von Anomalien“ überwacht und blockiert Aktionen, die für Computer des Unternehmensnetzwerks untypisch sind. Zur Überwachung von untypischen Aktionen verwendet die „Adaptive Kontrolle von Anomalien“ eine Auswahl von Regeln (z. B. die Regel *Start von Windows PowerShell aus einem Office-Programm*). Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt. Sie können ein Verhalten der „Adaptiven Kontrolle von Anomalien“ für jede einzelne Regeln auswählen und beispielsweise den Start von PowerShell-Skripten erlauben, um die Lösung von Unternehmensaufgaben zu automatisieren. Kaspersky Endpoint Security aktualisiert den Regelsatz aus den Programm-Datenbanken. Die Aktualisierung des Regelsatzes muss manuell bestätigt werden.

“Adaptive Kontrolle von Anomalien“ anpassen

Die Anpassung der „Adaptiven Kontrolle von Anomalien“ umfasst folgende Schritte:

1. Training der „Adaptiven Kontrolle von Anomalien“.

Nachdem die „Adaptive Kontrolle von Anomalien“ aktiviert ist, funktionieren die Regeln im *Lernmodus*. Im Verlauf des Trainings überwacht die „Adaptive Kontrolle von Anomalien“ die Auslösung von Regeln und sendet Auslöseereignisse an Kaspersky Security Center. Jede Regel hat eine eigene Dauer für den Lernmodus. Die Dauer des Lernmodus wird von den Kaspersky-Experten vorgegeben. Gewöhnlich dauert der Lernmodus 2 Wochen.

Wenn eine Regel während des Trainings nie ausgelöst wurde, betrachtet die „Adaptive Kontrolle von Anomalien“ die mit dieser Regel verbundenen Aktionen als untypisch. Kaspersky Endpoint Security blockiert alle Aktionen, die mit dieser Regel zusammenhängen.

Wenn eine Regel während des Trainings ausgelöst wurde, protokolliert Kaspersky Endpoint Security die Ereignisse im Bericht über ausgelöste Regeln und im Speicher **Auslösung von Regeln im Lernmodus**.

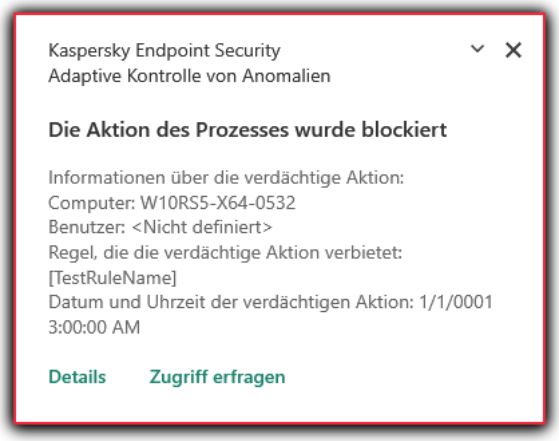
2. Analyse des Berichts über ausgelöste Regeln.

   Der Administrator analysiert den Bericht über ausgelöste Regeln oder den Inhalt des Speichers **Auslösung von Regeln im Lernmodus**. Anschließend kann der Administrator das Verhalten der „Adaptiven Kontrolle von Anomalien“ bei einer Auslösung der Regel festlegen: blockieren oder erlauben. Außerdem kann der Administrator die Regelauslösung weiterhin überwachen und die Dauer des Lernmodus für das Programm verlängern. Ergreift der Administrator keine Maßnahmen, so läuft das Programm ebenfalls im Lernmodus weiter. Die Dauer des Lernmodus beginnt von vorne.

Die „Adaptive Kontrolle von Anomalien“ wird im Echtzeitmodus angepasst. Die „Adaptive Kontrolle von Anomalien“ wird wie folgt angepasst:

- Die „Adaptive Kontrolle von Anomalien“ beginnt automatisch, jene Aktionen zu blockieren, die mit Regeln zusammenhängen, die im Lernmodus nicht ausgelöst wurden.
- Kaspersky Endpoint Security fügt neue Regeln hinzu oder löscht veraltete Regeln.
- Der Administrator passt die Verwendung der „Adaptiven Kontrolle von Anomalien“ nach der Analyse des Berichts über ausgelöste Regeln und des Inhalts des Speichers **Auslösung von Regeln im Lernmodus** an. Es wird empfohlen, den Bericht über ausgelöste Regeln und den Inhalt des Speichers **Auslösung von Regeln im Lernmodus zu überprüfen**.

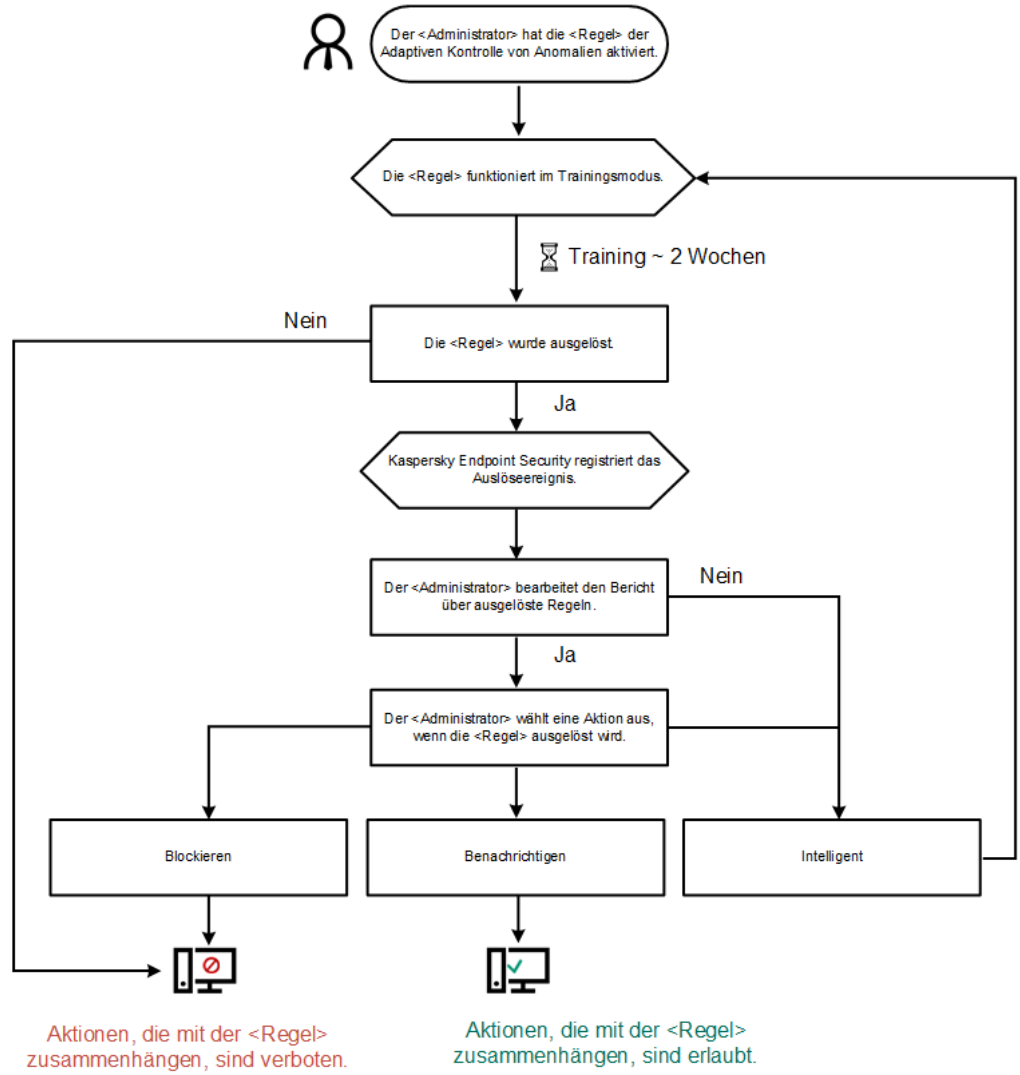
Wenn ein Schadprogramm versucht, eine Aktion auszuführen, blockiert Kaspersky Endpoint Security die Aktion und zeigt eine Benachrichtigung an (siehe Abbildung unten).



Benachrichtigung der „Adaptiven Kontrolle von Anomalien“

Algorithmus der „Adaptiven Kontrolle von Anomalien”

Um über die Ausführung einer Aktion, die mit einer Regeln verbunden ist, zu entscheiden, nutzt Kaspersky Endpoint Security den folgenden Algorithmus (siehe Abbildung unten).



Algorithmus der „Adaptiven Kontrolle von Anomalien"

Adaptive Kontrolle von Anomalien aktivieren und deaktivieren

Die Adaptive Kontrolle von Anomalien ist standardmäßig aktiviert.

Um die Adaptive Kontrolle von Anomalien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz** → **Sicherheitskontrolle** → **Adaptive Kontrolle von Anomalien** aus.
3. Verwenden Sie den Schalter **Adaptive Kontrolle von Anomalien**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Regel der Adaptiven Kontrolle von Anomalien aktivieren und deaktivieren

Um eine Regeln der Adaptiven Kontrolle von Anomalien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz → Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf die Schaltfläche **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Wählen Sie in der Tabelle einen Regelsatz aus (z. B. *Aktivität von Office-Programmen*) und erweitern Sie den Satz.
5. Wählen Sie eine Regel aus (z. B. *Windows PowerShell aus Office-Programme* starten).
6. Verwenden Sie den Schalter in der Spalte **Status**, um die „Adaptive Kontrolle von Anomalien“ zu aktivieren oder zu deaktivieren.
7. Speichern Sie die vorgenommenen Änderungen.

Aktion für den Fall, dass eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, ändern

Um die Aktion für den Fall, dass eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz → Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf die Schaltfläche **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Wählen Sie eine Regel in der Tabelle aus.
5. Klicken Sie auf **Ändern**.

   Das Eigenschaftenfenster der „Adaptive Kontrolle von Anomalien“-Regel wird geöffnet.
6. Wählen Sie im Block **Aktion** eine der folgenden Optionen aus:

   - **Intelligent** Bei Auswahl dieser Variante funktioniert die Regel der Adaptiven Kontrolle von Anomalien für den von den Kaspersky-Experten festgelegten Zeitraum im Lernmodus. Wenn in diesem Modus eine Regel der „Adaptiven Kontrolle von Anomalien“ ausgelöst wird, erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Eintrag im Speicher **Regelauslösung im Lernmodus des** Administrationsservers von Kaspersky Security Center. Nachdem der Zeitraum für den Lernmodus abgelaufen ist, blockiert Kaspersky Endpoint Security die Aktivität, die unter eine Regel der „Adaptiven Kontrolle von Anomalien“ fällt, und erstellt im Bericht einen Eintrag, der Informationen über diese Aktivität enthält.
   - **Blockieren** Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so blockiert Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

- **Informieren** Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

7. Speichern Sie die vorgenommenen Änderungen.

Um eine Ausnahme für eine „Adaptive Kontrolle von Anomalien"-Regel zu löschen, gehen Sie wie folgt vor:

Für die Regeln der Adaptiven Kontrolle von Anomalien können maximal 1.000 Ausnahmen erstellt werden. Es wird davon abgeraten, mehr als 200 Ausnahmen zu erstellen. Um die Anzahl der verwendeten Ausnahmen zu reduzieren, können in den Ausnahmeeinstellungen Masken angegeben werden.

Eine Ausnahme für eine Regel der „Adaptiven Kontrolle von Anomalien" enthält eine Beschreibung der Quell- und Zielobjekte. *Quellobjekt* – Objekt, das Aktionen ausführt. *Zielobjekt* – Objekt, mit dem Aktionen ausgeführt werden. Beispiel: Sie haben die Datei `file.xlsx` geöffnet. Als Ergebnis wird eine Bibliotheksdatei mit der DLL-Erweiterung in den Computerspeicher geladen. Diese Bibliothek wird von einem Browser verwendet (ausführbare Datei namens `browser.exe`). In diesem Beispiel ist `file.xlsx` das Quellobjekt, Excel der Quellprozess, `browser.exe` das Zielobjekt, und der Browser der Zielprozess.

Um eine Ausnahme für eine Regel der „Adaptiven Kontrolle von Anomalien" zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz** → **Sicherheitskontrolle** → **Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf die Schaltfläche **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Wählen Sie eine Regel in der Tabelle aus.
5. Klicken Sie auf **Ändern**.

   Das Eigenschaftenfenster der „Adaptive Kontrolle von Anomalien"-Regel wird geöffnet.
6. Klicken Sie im Fenster **Ausnahmen** auf **Hinzufügen**.

   Das Eigenschaftenfenster der Ausnahme wird geöffnet.
7. Wählen Sie den Benutzer aus, für den Sie eine Ausnahme konfigurieren möchten.

   Die „Adaptive Kontrolle von Anomalien" unterstützt keine Ausnahmen für Benutzergruppen. Wenn Sie eine Benutzergruppe auswählen, wendet Kaspersky Endpoint Security die Ausnahme nicht an.
8. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Ausnahme ein.
9. Geben Sie die Einstellungen des Quellobjekts oder des Quellprozesses an, die von dem Objekt gestartet wurden:

   - **Quellprozess**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`).

- **Hash des Quellprozesses**. Datei-Hash.
- **Quellobjekt**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`). Beispiel: Pfad der Datei `document.docm`, welche die Zielprozesse mithilfe eines Skripts oder Makros startet.

  Sie können auch andere Objekte für eine Ausnahme angeben, beispielsweise eine Webadresse, ein Makro, einen Befehl in der Befehlszeile, einen Registrierungspfad und andere. Geben Sie das Objekt nach der folgenden Vorlage an: `object://<Objekt>`, wobei `<Objekt>` für den Namen des Objekts steht. Beispiele: `object://web.site.example.com`, `object://VBA`, `object:\ipconfig`, `object://HKEY_USERS`. Sie können auch Masken verwenden, beispielsweise `object://*C:\Windows\temp\*`.
- **Hash des Quellobjekts**. Datei-Hash.

Die Regel für die „Adaptive Kontrolle von Anomalien“ erstreckt sich nicht auf die Aktionen, die von dem Objekt ausgeführt werden, oder auf Prozesse, die von dem Objekt gestartet werden.

10. Geben Sie die Einstellungen des Zielobjekts oder der Zielprozesse an, die mit dem Objekt ausgeführt wurden.
    - **Zielprozess**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`).
    - **Hash des Zielprozesses**. Datei-Hash.
    - **Zielobjekt**. Befehl zum Starten des Zielprozesses. Geben Sie den Befehl nach folgender Vorlage an `object://<Befehl>`, beispielsweise `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage.txt'"`. Sie können auch Masken verwenden, beispielsweise `object://*C:\windows\temp\*`.
    - **Hash des Zielobjekts**. Datei-Hash.

    Die Regel für die „Adaptive Kontrolle von Anomalien“ erstreckt sich nicht auf die Aktionen mit dem Objekt oder auf die Prozesse, die mit dem Objekt ausgeführt werden.
11. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Ausnahmen für die Regeln der „Adaptiven Kontrolle von Anomalien”

So exportieren oder importieren Sie die Liste der Ausnahmen für ausgewählte Regeln:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz → Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf die Schaltfläche **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Regeln aus, deren Ausnahmen Sie exportieren möchten.
   b. Klicken Sie auf **Export**.

c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

d. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.

e. Klicken Sie auf **Speichern**.

5. So importieren Sie die Liste der vertrauenswürdigen Geräte:

a. Klicken Sie auf **Import**.

b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

c. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. Speichern Sie die vorgenommenen Änderungen.

Updates für die Regeln der Adaptiven Kontrolle von Anomalien übernehmen

Neue Regeln der „Adaptiven Kontrolle von Anomalien“ können zur Regeltabelle hinzugefügt werden und vorhandene Regeln der „Adaptiven Kontrolle von Anomalien“ können abhängig vom Ergebnis des Updates der Antiviren-Datenbanken aus der Regeltabelle gelöscht werden. Kaspersky Endpoint Security markiert zu löschende und hinzuzufügende Regeln der „Adaptiven Kontrolle von Anomalien“ in der Tabelle, falls das Update für diese Regeln nicht übernommen wurde.

Bis ein Update übernommen wurde, zeigt Kaspersky Endpoint Security die Regeln der Adaptiven Kontrolle von Anomalien, die aufgrund des Updates gelöscht werden, in der Tabelle mit dem Status *Deaktiviert* an. Die Einstellungen dieser Regeln können nicht geändert werden.

Um ein Update für die Regeln der Adaptiven Kontrolle von Anomalien zu übernehmen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Programmkonfigurationsfenster **Schutz → Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.

3. Klicken Sie im Block **Regeln** auf die Schaltfläche **Regeln bearbeiten**.

Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.

4. Klicken Sie im geöffneten Fenster auf die Schaltfläche **Updates bestätigen**.

Die Schaltfläche **Updates bestätigen** ist verfügbar, wenn ein Update für die Regeln der Adaptiven Kontrolle von Anomalien vorliegt.

5. Speichern Sie die vorgenommenen Änderungen.

Meldungsvorlagen für die Adaptiven Kontrolle von Anomalien ändern

Wenn ein Benutzer versucht, eine Aktion auszuführen, die durch Regeln der „Adaptiven Kontrolle von Anomalien“ verboten ist, so meldet Kaspersky Endpoint Security, dass potentiell gefährliche Aktionen blockiert wurden. Wenn der Benutzer der Meinung ist, die Sperrung sei irrtümlich erfolgt, kann er aus der Sperrmeldung eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden.

Für Meldungen über die Sperrung von potentiell gefährlichen Aktionen sowie für die Nachricht an den Administrator sind Vorlagen vorgesehen. Die Meldungsvorlagen können geändert werden.

Gehen Sie folgendermaßen vor, um eine Meldungsvorlage zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Programmkonfigurationsfenster **Schutz → Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Adaptiven Kontrolle von Anomalien:
   - **Sperrung**. Vorlage der Nachricht an den Benutzer. Diese Nachricht wird angezeigt, wenn eine Regel der „Adaptiven Kontrolle von Anomalien“ ausgelöst wird, die eine untypische Aktion blockiert.
   - **Nachricht an den Administrator**. Vorlage der Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn eine Aktion nach Meinung des Benutzers irrtümlich blockiert wurde.
4. Speichern Sie die vorgenommenen Änderungen.

Berichte über die „Adaptive Kontrolle von Anomalien“ anzeigen

Um Berichte über die „Adaptive Kontrolle von Anomalien“ anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Adaptive Kontrolle von Anomalien** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Adaptive Kontrolle von Anomalien“ angezeigt.
6. Führen Sie eine der folgenden Aktionen aus:
   - Um einen Bericht über die Einstellungen der Regeln für die „Adaptive Kontrolle von Anomalien“ anzuzeigen, klicken Sie auf **Bericht über den Regelstatus**.

- Um einen Bericht über das Auslösen von Regeln der „Adaptiven Kontrolle von Anomalien“ anzuzeigen, klicken Sie auf **Bericht über ausgelöste Regeln**.

7. Der Vorgang zur Berichterstellung wird gestartet.

Der Bericht wird in einem neuen Fenster angezeigt.

Programmkontrolle

Die „Programmkontrolle“ verwaltet den Start von Programmen auf den Benutzercomputern. Dadurch wird ermöglicht, die Sicherheitsrichtlinie des Unternehmens bei der Verwendung von Programmen zu erfüllen. Außerdem reduziert die „Programmkontrolle“ das Risiko einer Infektion des Computers. Dazu wird der Zugriff auf Programme beschränkt.

Die „Programmkontrolle“ wird mit folgenden Schritten angepasst:

1. Programmkategorien erstellen

   Der Administrator erstellt Kategorien für die Programme, die er verwalten möchte. Die Programmkategorien gelten unabhängig von der Administrationsgruppe für alle Computer des Unternehmensnetzwerks. Für die Kategorien können Sie beispielsweise folgende Kriterien verwenden: KL-Kategorie (z. B. *Browser*), Datei-Hash und Programmhersteller.

2. Regeln der „Programmkontrolle“ erstellen.

   Der Administrator erstellt Regeln der „Programmkontrolle“ in der Richtlinie für die Administrationsgruppe. Eine Regel enthält Programmkategorien und einen Startstatus für die Programme aus diesen Kategorien: verboten oder erlaubt.

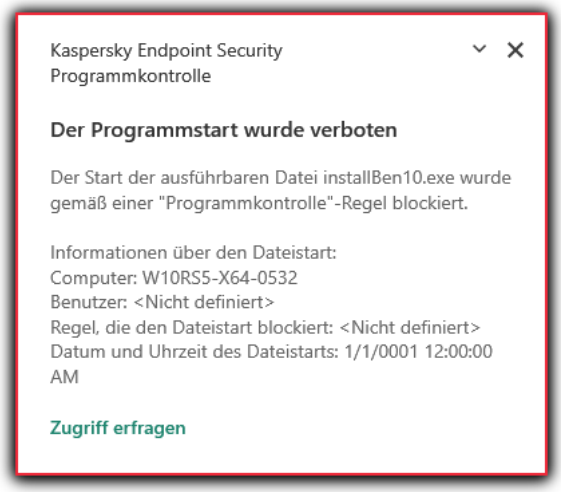
3. Modus der „Programmkontrolle“ auswählen.

   Der Administrator wählt einen Modus für die Arbeit mit den Programmen aus, die zu keiner Regel gehören: Denyliste und Allowliste.

Wenn der Benutzer versucht, ein verbotenes Programm zu starten, blockiert Kaspersky Endpoint Security den Programmstart und zeigt eine Benachrichtigung an (s. Abb. unten).

Die Einstellungen der „Programmkontrolle“ können im *Testmodus* überprüft werden. In diesem Modus führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Der Start von Programmen (auch von verbotenen Programmen) wird erlaubt.
- Beim Start eines verbotenen Programms wird eine entsprechende Benachrichtigung angezeigt und Informationen werden zum Bericht auf dem Benutzercomputer Informationen hinzugefügt.
- Daten über den Start verbotener Programme werden an Kaspersky Security Center gesendet.



Benachrichtigung der „Programmkontrolle"

Modi der „Programmkontrolle"

Die Komponente „Programmkontrolle" bietet zwei Modi:

- **Deny-Liste**. In diesem Modus erlaubt die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" verboten sind.

  Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

- **Allow-Liste**. In diesem Modus verbietet die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" erlaubt und nicht verboten sind.

  Wenn eine extrem genaue Erlaubnisregel für die Programmkontrolle erstellt wurde, verbietet die Komponente den Start aller neuen Programme, die noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet dabei aber die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Programme, die von Benutzern für dienstliche Zwecke benötigt werden.

  Beachten Sie die Tipps für die Anpassung von Regeln der Programmkontrolle im Allowlist-Modus.

Diese Modi für die Programmkontrolle können sowohl auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security als auch mithilfe von Kaspersky Security Center angepasst werden.

Allerdings verfügt Kaspersky Security Center über Tools, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht verfügbar sind und für folgende Aufgaben dienen:

- Programmkategorien erstellen

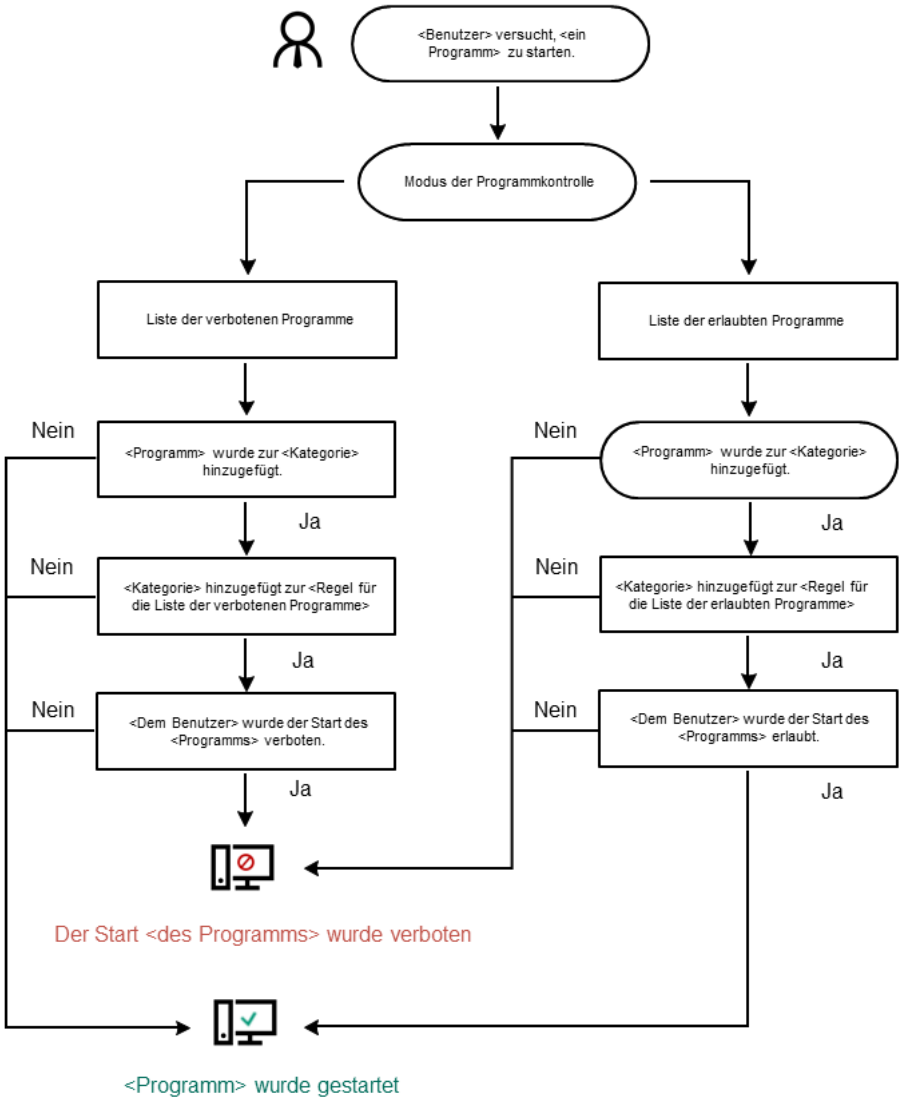
  Die Regeln der Programmkontrolle, die in der Verwaltungskonsole von Kaspersky Security Center erstellt wurden, beruhen auf den von Ihnen erstellten Programmkategorien, und nicht wie in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security auf ein- und ausschließenden Bedingungen.

- Empfang von Informationen über die Programme, die auf den Computern des lokalen Unternehmensnetzwerks installiert sind

Deshalb wird empfohlen, die Komponente „Programmkontrolle" mithilfe von Kaspersky Security Center anzupassen.

Algorithmus der „Programmkontrolle"

Kaspersky Endpoint Security verwendet einen Algorithmus, um über den Start eines Programms zu entscheiden (s. Abb. unten).



Algorithmus der „Programmkontrolle"

Funktionelle Beschränkungen der Programmkontrolle

Die Funktion der Komponente „Programmkontrolle" ist in folgenden Fällen beschränkt:

- Beim Programm-Upgrade wird der Import von Einstellungen für die Komponente „Programmkontrolle" nicht unterstützt.
- Beim Programm-Upgrade wird das Importieren der Einstellungen für die Komponente „Programmkontrolle" nur beim Upgrade von der Version Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher auf die Version Kaspersky Endpoint Security 11.6.0 für Windows unterstützt.

Beim Upgrade von anderen Programmversionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows muss die Komponente „Programmkontrolle" erneut angepasst werden, um die Funktionsfähigkeit der Komponente zu gewährleisten.

- Wenn keine Verbindung mit den KSN-Servern besteht, empfängt Kaspersky Endpoint Security die Informationen über die Reputation von Programmen und Modulen nur aus den lokalen Datenbanken.

  Abhängig davon, ob eine Verbindung mit den KSN-Servern besteht oder nicht, kann die Liste der Programme, die Kaspersky Endpoint Security zu der KL-Kategorie **Programme,die laut KSN-Reputation vertrauenswürdig sind** zuweist, unterschiedlich sein.

- Kaspersky Security Center kann Informationen über maximal 150.000 verarbeitete Dateien in der Datenbank speichern. Wenn diese Anzahl von Einträgen erreicht ist, werden neue Dateien nicht mehr verarbeitet. Um die Inventarisierung fortzusetzen, müssen von dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, Dateien gelöscht werden, die bisher bei der Inventarisierung in der Datenbank für Kaspersky Security Center aufgezeichnet worden sind.

- Der Start von Skripten wird von der Komponente nicht kontrolliert, wenn ein Skript nicht über die Befehlszeile an den Interpreter übermittelt wird.

  Ist der Start des Interpreters durch Regeln der Programmkontrolle erlaubt, so blockiert die Komponente ein Skript nicht, das aus diesem Interpreter gestartet wurde.

  Wenn die Regeln der Programmkontrolle mindestens den Start von einem der Skripte verbieten, die in der Interpreter-Befehlszeile angegeben sind, so blockiert die Komponente alle Skripte, die in der Interpreter-Befehlszeile angegeben sind.

- Der Start von Skripten aus Interpretern wird von der Komponente nicht kontrolliert, wenn der Interpreter vom Programm Kaspersky Endpoint Security nicht unterstützt wird.

  Kaspersky Endpoint Security unterstützt folgende Interpreter:

  - Java
  - PowerShell

  Es werden folgende Interpretertypen unterstützt:

  - %ComSpec%
  - %SystemRoot%\\system32\\regedit.exe
  - %SystemRoot%\\regedit.exe
  - %SystemRoot%\\system32\\regedt32.exe
  - %SystemRoot%\\system32\\cscript.exe
  - %SystemRoot%\\system32\\wscript.exe
  - %SystemRoot%\\system32\\msiexec.exe
  - %SystemRoot%\\system32\\mshta.exe
  - %SystemRoot%\\system32\\rundll32.exe;
  - %SystemRoot%\\system32\\wwahost.exe

- %SystemRoot%\\syswow64\\cmd.exe
- %SystemRoot%\\syswow64\\regedit.exe;
- %SystemRoot%\\syswow64\\regedt32.exe;
- %SystemRoot%\\syswow64\\cscript.exe;
- %SystemRoot%\\syswow64\\wscript.exe;
- %SystemRoot%\\syswow64\\msiexec.exe;
- %SystemRoot%\\syswow64\\mshta.exe;
- %SystemRoot%\\syswow64\\rundll32.exe;
- %SystemRoot%\\syswow64\\wwahost.exe

Programmkontrolle aktivieren und deaktivieren

Die „Programmkontrolle“ ist standardmäßig deaktiviert.

Um die Programmkontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Programmkontrolle** aus.
3. Verwenden Sie den Schalter **Programmkontrolle**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Programmkontrolle aktiviert ist, leitet das Programm daher Informationen über die Ausführung ausführbarer Dateien an das Kaspersky Security Center weiter. Sie können die Liste der laufenden ausführbaren Dateien im Kaspersky Security Center im Ordner **Ausführbare Dateien** anzeigen. Um Informationen über alle ausführbaren Dateien zu erhalten, anstatt nur ausführbare Dateien auszuführen, führen Sie die Aufgabe *Inventarisierung* aus.

Modus der Programmkontrolle auswählen

Um einen Modus für die Programmkontrolle auszuwählen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Programmkontrolle** aus.
3. Wählen Sie im Block **Modus "Kontrolle des Programmstarts"** eine der folgenden Optionen:
   - **Deny-Liste**. Bei Auswahl dieser Variante erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Verbotsregeln der

Programmkontrolle erfüllt sind.

- **Allow-Liste**. Bei Auswahl dieser Variante verbietet die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Erlaubnisregeln der Programmkontrolle erfüllt sind.

  Die Regeln **Goldene Kategorie** und **Vertrauenswürdige Programme mit Update-Funktionen** werden anfänglich für den Zulässigkeitslistenmodus definiert. Diese Regeln der Programmkontrolle entsprechen den KL-Kategorien. Zur KL-Kategorie „Goldene Kategorie“ gehören jene Programme, welche die normale Funktion des Betriebssystems gewährleisten. Zur KL-Kategorie „Vertrauenswürdige Programme mit Update-Funktionen“ gehören Programme mit Update-Funktionen der gängigen Softwarehersteller. Diese Regeln können nicht gelöscht werden. Die Einstellungen dieser Regeln können nicht geändert werden. Standardmäßig ist die Regel **Goldene Kategorie** aktiviert, und die Regel **Vertrauenswürdige Programme mit Update-Funktionen** ist deaktiviert. Der Start von Programmen, welche den Auslösebedingungen dieser Regeln entsprechen, ist für alle Benutzer erlaubt.

Wenn der Modus gewechselt wird, werden alle Regeln gespeichert, die in diesem Modus erstellt wurden. So ist eine erneute Verwendung der Regeln möglich. Um wieder zur Verwendung dieser Regeln zurückzukehren, brauchen Sie nur den erforderlichen Modus auszuwählen.

4. Wählen Sie im Abschnitt **Aktion beim Starten blockierter Programme** aus, welche Aktion die Komponente ausführen soll, wenn der Benutzer versucht, ein Programm auszuführen, das durch Regeln der Programmkontrolle blockiert ist.

5. Aktivieren Sie das Kontrollkästchen **Laden von DLL-Modulen kontrollieren**, damit Kaspersky Endpoint Security das Laden von DLL-Modulen kontrolliert, wenn die Benutzer Programme starten.

   Informationen über das Modul und das Programm, das dieses Modul geladen hat, werden im Bericht gespeichert.

   Kaspersky Endpoint Security kontrolliert nur jene DLL-Module und Treiber, die geladen wurden, nachdem das Kontrollkästchen aktiviert wurde. Starten Sie den Computer neu, nachdem das Kontrollkästchen aktiviert wurde. So wird gewährleistet, dass das Programm Kaspersky Endpoint Security alle DLL-Module und Treiber kontrolliert, also auch jene, die vor dem Start von Kaspersky Endpoint Security geladen wurden.

   Wenn die Funktion zur Kontrolle des Ladens von DLL-Modulen und Treibern aktiviert ist, vergewissern Sie sich, dass in den „Programmkontrolle“-Einstellungen entweder die Regel **Goldene Kategorie** aktiviert ist oder eine andere Regel, welche die KL-Kategorie „Vertrauenswürdige Zertifikate“ enthält und das Laden von DLL-Modulen und Treibern vor dem Start von Kaspersky Endpoint Security gewährleistet. Wenn die Kontrolle von DLL-Modulen und Treibern gleichzeitig mit der Regel **Goldene Kategorie** aktiviert ist, kann es zur Instabilität des Betriebssystems kommen.

   Es wird empfohlen, den Kennwortschutz für die Programmeinstellungen zu aktivieren, damit jene Verbotsregeln deaktiviert werden können, die den Start von DLL-Modulen und Treibern mit kritischer Priorität blockieren, ohne dazu die Richtlinieneinstellungen für Kaspersky Security Center zu ändern.

6. Speichern Sie die vorgenommenen Änderungen.

Arbeiten mit Regeln der Programmkontrolle in der Programmoberfläche

Kaspersky Endpoint Security überwacht mithilfe von Regeln die Versuche von Benutzern, Programme zu starten. Eine Regel der Programmkontrolle enthält Auslösebedingungen und legt die Aktionen fest, die von der Komponente „Programmkontrolle“ beim Auslösen der Regel ausgeführt werden (Erlaubnis oder Verbot des benutzerinitiierten Programmstarts).

Auslösebedingungen für eine Regel

Eine regelauslösende Bedingung hat folgenden Zusammenhang: „Art der Bedingung – Bedingungskriterium – Bedingungswert“. Basierend auf den Auslösebedingungen für eine Regel wendet Kaspersky Endpoint Security die Regel auf ein Programm an (oder wendet die Regel nicht an).

Die folgenden Arten von Bedingungen werden in Regeln verwendet:

- *Einschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel auf ein Programm an, wenn das Programm mindestens eine einschließende Bedingung erfüllt.
- *Ausschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel nicht auf ein Programm an, wenn das Programm mindestens eine ausschließende Bedingung oder keine einschließende Bedingung erfüllt.

Auslösebedingungen für eine Regel werden mithilfe von Kriterien definiert. Um in Kaspersky Endpoint Security Bedingungen zu erstellen, werden folgende Kriterien verwendet:

- Pfad des Ordners mit der ausführbaren Programmdatei oder Pfad der ausführbaren Programmdatei
- Metadaten: Name der ausführbaren Programmdatei, Version der ausführbaren Programmdatei, Programmname, Programmversion, Programmhersteller
- Hash der ausführbaren Programmdatei
- Zertifikat: Herausgeber, Subjekt, Fingerabdruck
- Zugehörigkeit eines Programms zu einer KL-Kategorie
- Speicherort der ausführbaren Programmdatei auf dem Wechseldatenträger

Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden. Entsprechen die Parameter eines zu startenden Programms den Werten von Kriterien, die in einer einschließenden Bedingung angegeben sind, so wird die Regel ausgelöst. In diesem Fall führt die Programmkontrolle die Aktion aus, die in der Regel angegeben ist. Entsprechen die Programmparameter den Werten von Kriterien, die in einer ausschließenden Bedingung angegeben sind, so überwacht die Programmkontrolle den Start des Programms nicht.

Entscheidungen der Komponente „Programmkontrolle“ beim Auslösen einer Regel

Wenn eine Regel ausgelöst wird, verfährt die Programmkontrolle nach der Regel und erlaubt oder verbietet den Benutzern (Benutzergruppen) den Programmstart. Sie können konkrete Benutzer oder Benutzergruppen wählen, denen der Start von Programmen, für welche eine Regel ausgelöst wird, erlaubt oder verboten werden soll.

In einer *Verbotsregel* ist kein Benutzer angegeben, dem der Start von Programmen erlaubt ist, welche die Regel erfüllen.

In einer *Erlaubnisregel* ist kein Benutzer angegeben, dem der Start von Programmen verboten ist, welche die Regel erfüllen.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Wenn für eine Benutzergruppe beispielsweise eine Erlaubnisregel der Programmkontrolle festgelegt ist, für einen Benutzer dieser Gruppe aber eine Verbotsregel der Programmkontrolle vorliegt, so wird der Start des Programms für diesen Benutzer verboten.

Status einer Regel

Für die Regeln der Programmkontrolle gibt es folgende Statusvarianten:

- **Aktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ verwendet wird.
- **Deaktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ ignoriert wird.
- **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche die Regel gilt, erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Regel der Programmkontrolle hinzufügen

So fügen Sie eine Regel der Programmkontrolle hinzu:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Programmkontrolle** aus.
3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.
4. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.
5. Definieren Sie auf der Registerkarte **Allgemeine Einstellungen** die Haupteinstellungen der Regel:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Regel ein.

   c. Erstellen oder ändern Sie eine Liste der Benutzer und/oder Benutzergruppen, denen erlaubt oder verboten wird, Programme zu starten, welche die Auslösebedingungen der Regel erfüllen. Klicken Sie dazu in der Tabelle **Subjekte und deren Rechte** auf **Hinzufügen**.

   Die Benutzerliste enthält standardmäßig den Wert **Alle**. Die Regel gilt für alle Benutzer.

   > Ist in der Tabelle kein Benutzer angegeben, so kann die Regel nicht gespeichert werden.

   d. Definieren Sie in der Tabelle **Subjekte und deren Rechte** mit dem Schalter die Berechtigung der Benutzer, Programme zu starten.

   e. Aktivieren Sie das Kontrollkästchen **Für die übrigen Benutzer verbieten**, damit das Programm den Start von Programmen, welche die Auslösebedingungen der Regel erfüllen, für alle Benutzer verbietet, die nicht in der

Spalte **Subjekt** angegeben sind und die nicht zu den in der Spalte **Subjekt** angegebenen Benutzergruppen gehören.

Ist das Kontrollkästchen **Für andere Benutzer verbieten** deaktiviert, so kontrolliert Kaspersky Endpoint Security den Start von Programmen für jene Benutzer nicht, die nicht in der Tabelle **Subjekte und deren Rechte** angegeben sind und die nicht zu den in der Tabelle **Subjekte und deren Rechte** angegebenen Benutzergruppen gehören.

f. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Programme, welche die Auslösebedingungen der Regel erfüllen, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet werden, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

6. Erstellen oder bearbeiten Sie auf der Registerkarte **Bedingungen** die Liste der Einschlussbedingungen für das Auslösen der Regel.

7. Erstellen oder bearbeiten Sie auf der Registerkarte **Ausnahmen** die Liste der Ausschlussbedingungen für das Auslösen der Regel.

   Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.

8. Speichern Sie die vorgenommenen Änderungen.

Auslösebedingung für eine Regel der Programmkontrolle hinzufügen

Um eine neue Auslösebedingung zu einer Regel der Programmkontrolle hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Programmkontrolle** aus.

3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.

4. Wählen Sie die Regel aus, für die Sie eine Auslösebedingung konfigurieren möchten.

   Die Eigenschaften für die Regel der Programmkontrolle werden geöffnet.

5. Wählen Sie die Registerkarte **Bedingungen** oder **Ausnahmen** und klicken Sie auf die Schaltfläche **Hinzufügen**.

6. Wählen Sie die Auslösebedingungen für die Regel der Programmkontrolle:

   - **Bedingungen aus den Eigenschaften der gestarteten Programme**. In der Liste der laufenden Programme können Sie die Programme auswählen, auf die die Regel der Programmkontrolle angewendet wird. Kaspersky Endpoint Security listet auch Programme auf, die zuvor auf dem Computer ausgeführt wurden. Sie müssen das Kriterium auswählen, das Sie zum Erstellen einer oder mehrerer Regel-Auslösebedingungen verwenden möchten: **Datei-Hash-Code**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Ordnerpfad**.

   - **Bedingungen „KL-Kategorie"**. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. So enthält die KL-Kategorie „Office-Programme" beispielsweise Programme aus den Paketen Microsoft Office, Adobe® Acrobat® und anderen.

- **Benutzerdefinierte Bedingung**. Sie können die Programmdatei und eine der Regel-Auslösebedingungen auswählen: **Datei-Hashcode**, **Zertifikat**, **Metadaten** oder **Pfad zu Datei oder Ordner**.

- **Bedingung nach Dateilaufwerk (Wechseldatenträger)**. Die Regel der Programmkontrolle wird nur auf Dateien angewendet, die auf einem Wechseldatenträger ausgeführt werden.

- **Bedingungen aus den Dateieigenschaften des angegebenen Ordners**. Die Regel der Programmkontrolle wird nur auf Dateien angewendet, die sich innerhalb des angegebenen Ordners befinden. Sie können auch Dateien aus Unterordnern einschließen oder ausschließen. Sie müssen das Kriterium auswählen, das Sie zum Erstellen einer oder mehrerer Regel-Auslösebedingungen verwenden möchten: **Datei-Hash-Code**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Ordnerpfad**.

7. Speichern Sie die vorgenommenen Änderungen.

Bitte beachten Sie beim Hinzufügen von Bedingungen die folgenden besonderen Überlegungen zur Programmkontrolle:

- Kaspersky Endpoint Security unterstützt den MD5-Dateihash nicht und kontrolliert den Start von Programmen nicht auf Basis des MD5-Hashs. Als Auslösebedingung für eine Regel wird der SHA256-Hash verwendet.

- Es wird davor gewarnt, als Auslösebedingungen für Regeln nur die Kriterien **Aussteller** und **Subjekt** zu verwenden. Die Verwendung dieser Kriterien ist unzuverlässig.

- Wenn Sie im Feld **Datei- oder Ordnerpfad** einen symbolischen Link verwenden, wird empfohlen, den symbolischen Link aufzulösen, damit die Regel der Programmkontrolle korrekt funktioniert. Klicken Sie dazu auf **Symbolischen Link auflösen**.

Status einer Regel der Programmkontrolle ändern

Um den Status einer Regel der Programmkontrolle zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Programmkontrolle** aus.

3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.

4. Öffnen Sie in der Spalte **Status** das Kontextmenü und wählen Sie einen der folgenden Punkte aus:

   - **Aktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.

   - **Deaktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.

   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche diese Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

5. Speichern Sie die vorgenommenen Änderungen.

Verwaltung von Regeln der Programmkontrolle im Kaspersky Security Center

Kaspersky Endpoint Security überwacht mithilfe von Regeln die Versuche von Benutzern, Programme zu starten. Eine Regel der Programmkontrolle enthält Auslösebedingungen und legt die Aktionen fest, die von der Komponente „Programmkontrolle“ beim Auslösen der Regel ausgeführt werden (Erlaubnis oder Verbot des benutzerinitiierten Programmstarts).

Auslösebedingungen für eine Regel

Eine regelauslösende Bedingung hat folgenden Zusammenhang: „Art der Bedingung – Bedingungskriterium – Bedingungswert“. Basierend auf den Auslösebedingungen für eine Regel wendet Kaspersky Endpoint Security die Regel auf ein Programm an (oder wendet die Regel nicht an).

Die folgenden Arten von Bedingungen werden in Regeln verwendet:

- *Einschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel auf ein Programm an, wenn das Programm mindestens eine einschließende Bedingung erfüllt.
- *Ausschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel nicht auf ein Programm an, wenn das Programm mindestens eine ausschließende Bedingung oder keine einschließende Bedingung erfüllt.

Auslösebedingungen für eine Regel werden mithilfe von Kriterien definiert. Um in Kaspersky Endpoint Security Bedingungen zu erstellen, werden folgende Kriterien verwendet:

- Pfad des Ordners mit der ausführbaren Programmdatei oder Pfad der ausführbaren Programmdatei
- Metadaten: Name der ausführbaren Programmdatei, Version der ausführbaren Programmdatei, Programmname, Programmversion, Programmhersteller
- Hash der ausführbaren Programmdatei
- Zertifikat: Herausgeber, Subjekt, Fingerabdruck
- Zugehörigkeit eines Programms zu einer KL-Kategorie
- Speicherort der ausführbaren Programmdatei auf dem Wechseldatenträger

Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden. Entsprechen die Parameter eines zu startenden Programms den Werten von Kriterien, die in einer einschließenden Bedingung angegeben sind, so wird die Regel ausgelöst. In diesem Fall führt die Programmkontrolle die Aktion aus, die in der Regel angegeben ist. Entsprechen die Programmparameter den Werten von Kriterien, die in einer ausschließenden Bedingung angegeben sind, so überwacht die Programmkontrolle den Start des Programms nicht.

Entscheidungen der Komponente „Programmkontrolle“ beim Auslösen einer Regel

Wenn eine Regel ausgelöst wird, verfährt die Programmkontrolle nach der Regel und erlaubt oder verbietet den Benutzern (Benutzergruppen) den Programmstart. Sie können konkrete Benutzer oder Benutzergruppen wählen, denen der Start von Programmen, für welche eine Regel ausgelöst wird, erlaubt oder verboten werden soll.

In einer *Verbotsregel* ist kein Benutzer angegeben, dem der Start von Programmen erlaubt ist, welche die Regel erfüllen.

In einer *Erlaubnisregel* ist kein Benutzer angegeben, dem der Start von Programmen verboten ist, welche die Regel erfüllen.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Wenn für eine Benutzergruppe beispielsweise eine Erlaubnisregel der Programmkontrolle festgelegt ist, für einen Benutzer dieser Gruppe aber eine Verbotsregel der Programmkontrolle vorliegt, so wird der Start des Programms für diesen Benutzer verboten.

Status einer Regel

Für die Regeln der Programmkontrolle gibt es folgende Statusvarianten:

- **Aktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ verwendet wird.
- **Deaktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ ignoriert wird.

Test. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche die Regel gilt, erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Empfang von Informationen über die Programme, die auf Benutzercomputern installiert sind

Um optimale Regeln der Programmkontrolle zu erstellen, sollte bekannt sein, welche Programme auf den Computern des lokalen Unternehmensnetzwerks eingesetzt werden. Dazu können Sie folgende Informationen erhalten:

- Hersteller, Versionen und Sprachversionen der Programme, die im lokalen Unternehmensnetzwerk verwendet werden
- Häufigkeit von Programm-Updates
- im Unternehmen geltende Richtlinien für die Nutzung von Programmen (Dies können Sicherheitsrichtlinien oder administrative Richtlinien sein.)
- Speicherort für Programmpakete

Um Informationen über die Programme zu erhalten, die auf den Computern des lokalen Unternehmensnetzwerks im Einsatz sind, können Sie Daten aus den Ordnern **Programm-Registry** und **Ausführbare Dateien** verwenden. Die Ordner **Programm-Registry** und **Ausführbare Dateien** gehören zum Ordner **Programmverwaltung** in der Verwaltungskonsolenstruktur von Kaspersky Security Center.

Der Ordner **Programmverzeichnis** enthält eine Liste von Programmen, die der Administrationsagent auf den Client-Computern gefunden hat, auf denen er installiert ist.

Der Ordner **Ausführbare Dateien** enthält eine Liste mit den ausführbaren Dateien, die bisher auf dem Client-Computern gestartet oder bei einer Inventarisierungsaufgabe für Kaspersky Endpoint Security gefunden wurden.

Im Eigenschaftenfenster eines gewählten Programms finden Sie im Ordner **Programm-Registry** oder **Ausführbare Dateien** allgemeine Informationen über das Programm und über seine ausführbaren Dateien. Außerdem steht eine Liste der Computer bereit, auf denen dieses Programm installiert ist.

*Um das Fenster mit den Programmeigenschaften im Ordner **Programm-Registry** zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert → Programmverwaltung → Programm-Registry** aus.
3. Wählen Sie ein Programm aus.
4. Wählen Sie im Kontextmenü des Programms den Punkt **Eigenschaften** aus.

*Um das Eigenschaftenfenster der ausführbaren Datei im Ordner **Ausführbare Dateien** zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Programmverwaltung → Ausführbare Dateien** aus.
3. Wählen Sie eine ausführbare Datei aus.
4. Wählen Sie im Kontextmenü der ausführbaren Datei den Punkt **Eigenschaften** aus.

Programmkategorien erstellen

Um das Anlegen von Regeln der Programmkontrolle zu vereinfachen, können Sie Programmkategorien erstellen.

Es wird empfohlen, die Kategorie „Programme für die Arbeit“ zu erstellen und eine Standardauswahl von Programmen in diese Kategorie aufzunehmen, die im Unternehmen eingesetzt werden. Falls bestimmte Benutzergruppen unterschiedliche Programmsets einsetzen, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

Um eine Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Programmverwaltung → Programmkategorie** aus.
3. Klicken Sie im Arbeitsbereich auf **Kategorie erstellen**.

   Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer benutzerdefinierten Kategorie.

Schritt 1. Kategorietyp auswählen

Wählen Sie bei diesem Schritt einen der folgenden Typen für die Programmkategorien aus:

- **Manuell zu erweiternde Kategorie**. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim Schritt „Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest“ und beim Schritt „Legen Sie die Bedingungen für den Ausschluss der Programme aus der Kategorie fest“ die Kriterien festlegen, nach denen ausführbare Dateien in die Kategorie aufgenommen werden sollen.

- **Kategorie für ausführbare Dateien der gewählten Geräte**. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim Schritt „Einstellungen“ einen Computer angeben, dessen ausführbare Dateien automatisch in diese Kategorie aufgenommen werden sollen.

- **Kategorie für ausführbare Dateien aus dem angegebenen Ordner**. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim Schritt „Ordner der Datenverwaltung“ einen Ordner angeben, aus dem ausführbare Dateien automatisch in die Kategorie aufgenommen werden sollen.

Wenn eine automatisch zu erweiternde Kategorie erstellt wird, führt Kaspersky Security Center die Inventarisierung für Dateien der folgenden Formate aus: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Schritt 2. Geben Sie den Namen der Benutzerkategorie ein.

Geben Sie bei diesem Schritt einen Namen für die Programmkategorie an.

Schritt 3. Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** die Bedingungen aus, nach denen Programme in diese Kategorie aufgenommen werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.

- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.

- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Hash-Werte der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Zertifikate der Dateien im Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck des Zertifikats** nicht angegeben ist.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Paket aus. Die Metadaten der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Paket aus. Die Hashs der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie „Office-Programme“ gehören beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Programmordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Kategorie auf.

- **Zertifikate aus der Zertifikatsdatenverwaltung**. Wählen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie die Zertifikate aus, mit denen die ausführbaren Dateien signiert sind.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck des Zertifikats** nicht angegeben ist.

- **Datenträgertyp**. Geben Sie den Typ des Massenspeichergerätes (alle Festplatten und Wechseldatenträger oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Schritt 4. Legen Sie die Bedingungen für den Ausschluss der Programme aus der Kategorie fest.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Die Programme, die bei diesem Schritt angegeben werden, werden auch dann aus der Kategorie ausgeschlossen, wenn diese Programme beim Schritt „Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest“ angegeben wurden.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** die Bedingungen aus, nach denen Programme aus dieser Kategorie ausgeschlossen werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.

- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.

- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Hash-Werte der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Zertifikate der Dateien im Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Paket aus. Die Metadaten der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Paket aus. Die Hashs der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie „Office-Programme" gehören beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Programmordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Kategorie auf.

- **Zertifikate aus der Zertifikatsdatenverwaltung**. Wählen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie die Zertifikate aus, mit denen die ausführbaren Dateien signiert sind.

- **Datenträgertyp**. Geben Sie den Typ des Massenspeichergerätes (alle Festplatten und Wechseldatenträger oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Schritt 5. Einstellungen

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien der gewählten Geräte** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Hinzufügen** und geben Sie die Computer an, deren ausführbare Dateien Kaspersky Security Center in die Programmkategorie aufnehmen soll. Kaspersky Security Center fügt der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzu, die sich im Ordner **Ausführbare Dateien** befinden.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Algorithmus zur Berechnung der Hash-Funktion durch das Programm Kaspersky Security Center Um einen Algorithmus auszuwählen, muss mindestens eines der folgenden Kontrollkästchen aktiviert werden:

  - **SHA-256 für die Dateien der Kategorie berechnen (wird unterstützt für die Version Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)**.

  - **MD5 für die Dateien der Kategorie berechnen (wird unterstützt für ältere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

- Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center die Programmkategorie regelmäßig bereinigt und zu

der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

Ist das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren** deaktiviert ist, so nimmt Kaspersky Security Center nach der Erstellung der Programmkategorie in dieser Kategorie keine Änderungen vor.

- Feld **Untersuchungsintervall (Std.)**. In diesem Feld können Sie den Zeitraum (in Stunden) angeben, nach dessen Ablauf Kaspersky Security Center die Programmkategorie bereinigt und zu der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

  Das Feld ist verfügbar, wenn das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren** aktiviert ist.

Schritt 6. Ordner der Datenverwaltung

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien aus dem angegebenen Ordner** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Durchsuchen** und geben Sie einen Ordner an, den Kaspersky Security Center nach ausführbaren Dateien durchsuchen soll, um diese automatisch zu der Programmkategorie hinzuzufügen.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Kontrollkästchen **Dynamic Link Libraries (.dll) zur Kategorie hinzufügen**. Aktivieren Sie das Kontrollkästchen, damit dynamische Programmbibliotheken (Dateien mit dem Format DLL) in die Programmkategorie aufgenommen werden.

  Wenn Dateien im DLL-Format in die Programmkategorie aufgenommen werden, kann sich die Leistungsfähigkeit von Kaspersky Security Center vermindern.

- Kontrollkästchen **Daten zu Skripten in die Kategorie aufnehmen**. Aktivieren Sie das Kontrollkästchen, damit Skripte in die Programmkategorie aufgenommen werden.

  Wenn Skripte in die Programmkategorie aufgenommen werden, kann die Leistungsfähigkeit von Kaspersky Security Center sinken.

- Algorithmus zur Berechnung der Hash-Funktion durch das Programm Kaspersky Security Center Um einen Algorithmus auszuwählen, muss mindestens eines der folgenden Kontrollkästchen aktiviert werden:

  - **SHA-256 für die Dateien der Kategorie berechnen (wird unterstützt für die Version Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)**.

  - **MD5 für die Dateien der Kategorie berechnen (wird unterstützt für ältere Versionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

- Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, regelmäßig nach ausführbaren Dateien durchsucht.

  Ist das Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen** deaktiviert, so durchsucht Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, nur dann, wenn der Ordner geändert wurde, ihm Dateien hinzugefügt oder Dateien daraus gelöscht wurden.

- Feld **Untersuchungsintervall (Std.)**. In diesem Feld können Sie angeben, nach welchem Zeitraum (in Stunden) Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, durchsuchen soll.

  Das Feld ist verfügbar, wenn das Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen** aktiviert ist.

Schritt 7. Benutzerkategorie erstellen

Um den Installationsassistenten abzuschließen, klicken Sie auf **Fertig**.

Ausführbare Dateien aus dem Ordner „Ausführbare Dateien“ zu einer Programmkategorie hinzufügen

Im Ordner **Ausführbare Dateien** wird eine Liste der ausführbaren Dateien angezeigt, die auf den Computern gefunden wurden. Kaspersky Endpoint Security erstellt die Liste der ausführbaren Dateien nach der Ausführung der Inventarisierungsaufgabe.

*Um die ausführbaren Dateien aus dem Ordner **Ausführbare Dateien** zu der Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert** → **Programmverwaltung** → **Ausführbare Dateien** aus.
3. Wählen Sie im Arbeitsbereich die ausführbaren Dateien aus, die Sie zu der Programmkategorie hinzufügen möchten.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für die ausgewählten ausführbaren Dateien und wählen Sie den Punkt **Zur Kategorie hinzufügen** aus.

   Das Fenster **Programmkategorie auswählen** wird geöffnet.
5. Führen Sie im Fenster **Programmkategorie auswählen** folgende Aktionen aus:
   - Wählen Sie im oberen Fensterbereich eine der folgenden Varianten aus:
     - **Programmkategorie erstellen**. Wählen Sie diese Variante aus, wenn Sie eine neue Programmkategorie erstellen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.
     - **Regeln zur angegebenen Kategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine vorhandene Programmkategorie auswählen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.
   - Wählen Sie im Block **Regeltyp** eine der folgenden Varianten aus:
     - **Zu den Aufnahmeregeln hinzufügen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien zu einer Programmkategorie hinzugefügt werden.
     - **Zu den Ausnahmeregeln hinzufügen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien aus einer Programmkategorie ausgeschlossen werden.
   - Wählen Sie im Block **Typ der Dateiinformationen** eine der folgenden Varianten aus:

- **Zertifikatdaten (oder SHA-256 für Dateien ohne Zertifikat)**.
- **Zertifikatdaten (Dateien ohne Zertifikat werden übersprungen)**
- **Nur SHA-256 (Dateien ohne SHA-256 werden übersprungen)**
- **Nur MD5 (für die Kompatibilität mit Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Klicken Sie auf **OK**.

Ausführbare Dateien, die mit Ereignissen zusammenhängen, zu einer Programmkategorie hinzufügen

Um ausführbare Dateien, die mit Ereignissen der „Programmkontrolle" zusammenhängen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.
3. Wählen Sie in der Dropdown-Liste **Ereignisse für Auswahl** eine Auswahl von Ereignissen über die Verwendung der Komponente „Programmkontrolle" aus (Ereignisse aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle" anzeigen, Ereignisse aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle" anzeigen).
4. Klicken Sie auf **Auswahl starten**.
5. Wählen Sie die Ereignisse aus, für welche ausführbare Dateien zu der Programmkategorie hinzugefügt werden sollen.
6. Öffnen Sie durch Rechtsklick das Kontextmenü für die ausgewählten Ereignisse und wählen Sie den Punkt **Zur Kategorie hinzufügen** aus.

   Das Fenster **Programmkategorie auswählen** wird geöffnet.
7. Führen Sie im Fenster **Programmkategorie auswählen** folgende Aktionen aus:
   - Wählen Sie im oberen Fensterbereich eine der folgenden Varianten aus:
     - **Programmkategorie erstellen**. Wählen Sie diese Variante aus, wenn Sie eine neue Programmkategorie erstellen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.
     - **Regeln zur angegebenen Kategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine vorhandene Programmkategorie auswählen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.
   - Wählen Sie im Block **Regeltyp** eine der folgenden Varianten aus:
     - **Zu den Aufnahmeregeln hinzufügen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien zu einer Programmkategorie hinzugefügt werden.
     - **Zu den Ausnahmeregeln hinzufügen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien aus einer Programmkategorie ausgeschlossen werden.

- Wählen Sie im Block **Typ der Dateiinformationen** eine der folgenden Varianten aus:
  - **Zertifikatdaten (oder SHA-256 für Dateien ohne Zertifikat)**.
  - **Zertifikatdaten (Dateien ohne Zertifikat werden übersprungen)**
  - **Nur SHA-256 (Dateien ohne SHA-256 werden übersprungen)**
  - **Nur MD5 (für die Kompatibilität mit Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Klicken Sie auf **OK**.

Regeln der Programmkontrolle mithilfe von Kaspersky Security Center hinzufügen und ändern

Um mithilfe von Kaspersky Security Center eine Regel für die Programmkontrolle hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle“ angezeigt.
6. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, wenn Sie eine Regel hinzufügen möchten.
   - Wenn Sie eine vorhandene Regel ändern möchten, wählen Sie in der Liste eine Regel und klicken Sie auf **Ändern**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.
7. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie eine neue Kategorie erstellen möchten, gehen Sie wie folgt vor:
     a. Klicken Sie auf **Kategorie erstellen**.

        Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.
     b. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer benutzerdefinierten Kategorie.
     c. Wählen Sie aus der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus.
   - Wenn Sie eine vorhandene Kategorie ändern möchten, gehen Sie wie folgt vor:

a. Wählen Sie in der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus, die Sie ändern möchten.

b. Klicken Sie auf **Eigenschaften**.

Das Fenster **Eigenschaften <Name der Kategorie>** wird geöffnet.

c. Ändern Sie die Einstellungen der ausgewählten Programmkategorie.

d. Klicken Sie auf **OK**.

e. Wählen Sie in der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus, auf deren Basis Sie eine Regel erstellen möchten.

8. Klicken Sie in der Tabelle **Subjekte und deren Rechte** auf **Hinzufügen**.

Das Windows-Standardfenster **Auswahl: „Benutzer“ oder „Gruppen”** wird geöffnet.

9. Legen Sie im Fenster **Auswahl: „Benutzer“ oder „Gruppen”** eine Liste mit Benutzern und/oder Benutzergruppen an, für welche Sie die Möglichkeit zum Starten von Programm, die zur ausgewählten Kategorie gehören, anpassen möchten.

10. Gehen Sie in der Tabelle **Subjekte und deren Rechte** wie folgt vor:

- Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu erlauben, aktivieren Sie das Kontrollkästchen **Erlauben** in den entsprechenden Zeilen.
- Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu verbieten, aktivieren Sie das Kontrollkästchen **Verbieten** in den entsprechenden Zeilen.

11. Aktivieren Sie das Kontrollkästchen **Für andere Benutzer verbieten**, damit das Programm den Start von Programmen aus der gewählten Kategorie für alle Benutzer verbietet, die nicht in der Spalte **Subjekt** angegeben sind und die nicht zu den in der Spalte **Subjekt** angegebenen Benutzergruppen gehören.

12. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Programme, welche zu der ausgewählten Programmkategorie gehören, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet werden, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.

13. Speichern Sie die vorgenommenen Änderungen.

Ändern des Status einer Regel der Programmkontrolle mithilfe von Kaspersky Security Center

Um den Status einer Regel der Programmkontrolle zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

5. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle“ angezeigt.

6. Öffnen Sie in der Spalte **Status** durch Linksklick das Kontextmenü und wählen Sie einen der folgenden Punkte aus:

   - **Aktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ verwendet wird.
   - **Deaktiviert**. Dieser Status bedeutet, dass diese Regel von der Komponente „Programmkontrolle“ ignoriert wird.
   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

     Mithilfe des Status **Test** können Sie für einen Teil der Regeln die Aktion festlegen, die dem Element **Regeln testen** entspricht, wenn in der Dropdown-Liste **Aktion** das Element **Regeln anwenden** ausgewählt ist.

7. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Regeln der Programmkontrolle

Sie können die Liste der Regeln der Programmkontrolle in eine XML-Datei exportieren. Mit der Export-/Importfunktion können Sie die Liste der Regeln der Programmkontrolle sichern oder die Liste auf einen anderen Server migrieren.

Wenn Sie Regeln der „Programmkontrolle“ exportieren und importieren, beachten Sie bitte die folgenden Sonderbedingungen:

- Kaspersky Endpoint Security exportiert die Regelliste nur für den momentan aktiven „Programmkontrolle“-Modus. Das bedeutet, wenn die „Programmkontrolle“ im Deny-Liste-Modus läuft, exportiert Kaspersky Endpoint Security nur die Regeln für diesen Modus. Um die Regelliste für den Allow-Liste-Modus zu exportieren, müssen Sie den Modus ändern und den Exportvorgang erneut ausführen.
- Kaspersky Endpoint Security verwendet Programmkategorien für die „Programmkontrolle“. Wenn Sie die Liste der „Programmkontrolle“-Regeln auf einen anderen Server migrieren, müssen Sie auch die Liste der Programmkategorien migrieren. Mehr Details über den Export und Import von Programmkategorien *finden Sie in der Hilfe für Kaspersky Security Center*.

Exportieren und Importieren einer Liste von Regeln der Programmkontrolle in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Programmkontrolle** aus.
6. So ändern Sie den Status einer Regel der Programmkontrolle:
   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
7. So exportieren Sie eine Liste der Regeln der Programmkontrolle:
   a. Klicken Sie auf **Import**.
      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

[Exportieren und Importieren einer Liste von Regeln der Programmkontrolle in der Web Console und der Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste der Regeln exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Sicherheitskontrollen → Programmkontrolle**.
5. Klicken Sie auf den Link **Einstellungen für Regellisten**.
6. Wählen Sie eine Liste mit Regeln aus: Programm-Denyliste oder -Allowliste.
7. So ändern Sie den Status einer Regel der Programmkontrolle:
   a. Wählen Sie die Regeln, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Regeln exportieren möchten, oder exportieren Sie die gesamte Liste.
   d. Klicken Sie auf **Export**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine XML-Datei im Standard-Download-Ordner.
8. So exportieren Sie eine Liste der Regeln der Programmkontrolle:
   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
9. Speichern Sie die vorgenommenen Änderungen.

Regeln der Programmkontrolle mithilfe von Kaspersky Security Center testen

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Test für Regeln der Programmkontrolle zu aktivieren und ihre Funktion zu analysieren. Wenn der Testlauf für die Regel der Programmkontrolle aktiviert ist, werden Programme, für welche der Start durch die Programmkontrolle verboten ist, von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Für die Funktionsanalyse von Regeln der Programmkontrolle müssen die Ereignisse aus den Ausführungsergebnissen der Komponente „Programmkontrolle“ überprüft werden, die bei Kaspersky Security Center eintreffen. Wenn im Testmodus für alle Programme, die der Benutzer zum Arbeiten benötigt, keine Ereignisse über ein Startverbot vorliegen, sind die Regeln korrekt. Andernfalls wird empfohlen, die Einstellungen der von Ihnen erstellten Regeln zu präzisieren, zusätzliche Regeln zu erstellen oder vorhandene Regeln zu löschen.

Kaspersky Endpoint Security erlaubt standardmäßig den Start aller Programme, unter Ausnahme von Programmen, die durch Regeln verboten sind.

Um in Kaspersky Security Center den Test für die Regeln der „Programmkontrolle“ zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle“ angezeigt.
6. Wählen Sie in der Dropdown-Liste **Kontrollmodus** eines der folgenden Elemente aus:

   - **Deny-Liste**. Bei Auswahl dieser Variante erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Verbotsregeln der Programmkontrolle erfüllt sind.
   - **Allow-Liste**. Bei Auswahl dieser Variante verbietet die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Erlaubnisregeln der Programmkontrolle erfüllt sind.
7. Führen Sie eine der folgenden Aktionen aus:

   - Um den Test für die Regeln der „Programmkontrolle“ zu aktivieren, wählen Sie in der Dropdown-Liste **Aktion** das Element **Regeln testen** aus.
   - Wenn Sie die „Programmkontrolle“ aktivieren möchten, um den Start von Programmen auf den Benutzercomputern zu verwalten, wählen Sie in der Dropdown-Liste **Aktion** das Element **Regeln anwenden** aus.
8. Speichern Sie die vorgenommenen Änderungen.

Ereignisse aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle“ anzeigen

Um die Ereignisse anzuzeigen, die als Ergebnisse des Testlaufs der Komponente „Programmkontrolle“ in Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.
3. Klicken Sie auf **Auswahl erstellen**.

   Das Fenster **Eigenschaften <Name der Auswahl>** wird geöffnet.
4. Öffnen Sie den Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle entfernen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** die Kontrollkästchen **Der Programmstart wurde im Testmodus verboten** und **Der Programmstart wurde im Testmodus erlaubt**.
7. Klicken Sie auf **OK**.
8. Wählen Sie in der Liste **Ereignisse für Auswahl** die erstellte Auswahl aus.
9. Klicken Sie auf **Auswahl starten**.

Bericht über im Testmodus verbotene Programme anzeigen

Um einen Bericht über im Testmodus verbotene Programme anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.
3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.
4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** die Variante **Andere → Bericht über im Testmodus verbotene Programme** aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.
5. Öffnen Sie den Bericht durch Doppelklick.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Ereignisse aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle“ anzeigen

Um die Ereignisse anzuzeigen, die aus den Ausführungsergebnissen der Komponente „Programmkontrolle“ stammen und in Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.
3. Klicken Sie auf **Auswahl erstellen**.

Das Fenster **Eigenschaften <Name der Auswahl>** wird geöffnet.

4. Öffnen Sie den Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle entfernen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** das Kontrollkästchen **Der Programmstart wurde verboten**.
7. Klicken Sie auf **OK**.
8. Wählen Sie in der Liste **Ereignisse für Auswahl** die erstellte Auswahl aus.
9. Klicken Sie auf **Auswahl starten**.

Bericht über verbotene Programme anzeigen

Um einen Bericht über verbotene Programme anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.
3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.
4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** die Variante **Andere → Bericht über verbotene Programme** aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.
5. Öffnen Sie den Bericht durch Doppelklick.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Regeln der Programmkontrolle testen

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Test für Regeln der Programmkontrolle zu aktivieren und ihre Funktion zu analysieren.

Für die Funktionsanalyse von Regeln der Programmkontrolle müssen die Ereignisse aus den Ausführungsergebnissen der Komponente „Programmkontrolle“ überprüft werden, die bei Kaspersky Security Center eintreffen. Wenn im Testmodus für alle Programme, die der Benutzer zum Arbeiten benötigt, keine Ereignisse über ein Startverbot vorliegen, sind die Regeln korrekt. Andernfalls wird empfohlen, die Einstellungen der von Ihnen erstellten Regeln zu präzisieren, zusätzliche Regeln zu erstellen oder vorhandene Regeln zu löschen.

Um den Test für die Regeln der Programmkontrolle zu aktivieren oder um eine Sperraktion der Programmkontrolle auszuwählen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz** → **Sicherheitskontrollen** → **Programmkontrolle** aus.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.

3. Wählen Sie in der Spalte **Status** die Option **Test**.

   Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche diese Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

4. Speichern Sie die vorgenommenen Änderungen.

Programme, für welche die Komponente „Programmkontrolle“ den Start verbietet, werden von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Aktivitätsmonitor für Programme

Der *Aktivitätsmonitor für Programme* dient dazu, in Echtzeit Informationen über die Aktivität von Programmen auf einem Benutzercomputer anzuzeigen.

Die Verwendung des „Aktivitätsmonitors für Programme“ erfordert die Installation der Komponenten „Programmkontrolle“ und „Programm-Überwachung“. Wenn diese Komponenten nicht installiert sind, ist der Abschnitt „Aktivitätsmonitor für Programme“ im Programmhauptfenster ausgeblendet.

Um den „Aktivitätsmonitor für Programme“ zu starten:

Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Aktivitätsmonitor für Programme**.

Das Fenster **Programmaktivität** wird geöffnet. Dieses Fenster enthält auf drei Registerkarten mit Informationen über die Aktivität von Programmen auf dem Benutzercomputer:

- Die Registerkarte **Alle Programme** enthält Informationen über alle Programme, die auf dem Computer installiert sind.
- Die Registerkarte **Wird ausgeführt** enthält Echtzeitinformationen über den Verbrauch der Computerressourcen durch die einzelnen Programme. Von dieser Registerkarte aus können Sie die Berechtigungen für ein bestimmtes Programm anpassen.
- Die Registerkarte **Beim Hochfahren starten** enthält eine Liste der Programme, die beim Betriebssystemstart gestartet werden.

Regeln für das Erstellen von Masken für Datei- oder Ordnernamen

Eine *Maske für den Datei- oder Ordnernamen* ist ein Platzhalter für einen Datei- oder Ordnernamen und für eine Dateierweiterung.

Für die Maske eines Datei- oder Ordnernamens sind folgende Platzhalter zulässig:

- Das Symbol `*` (Sternchen), das eine beliebige Zeichenkombination ersetzt (einschließlich einer leeren Zeichenfolge). Beispiel: Die Maske `C:\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung `txt`, die sich

in Ordnern und Unterordnern auf Laufwerk (C:) befinden.

- Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

Meldungsvorlagen für die Programmkontrolle ändern

Versucht ein Benutzer, ein Programm zu starten, das durch eine Regel der Programmkontrolle verboten ist, so meldet Kaspersky Endpoint Security, dass der Programmstart blockiert wurde. Wenn der Benutzer der Meinung ist, der Programmstart sei irrtümlich blockiert worden, kann der Benutzer aus der Sperrmeldung eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden.

Für die Meldung über die Sperrung des Programmstarts sowie für die Nachricht an den Administrator sind Vorlagen vorgesehen. Die Meldungsvorlagen können geändert werden.

Gehen Sie folgendermaßen vor, um eine Meldungsvorlage zu ändern:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen die Option **Schutz → Sicherheitskontrollen → Programmkontrolle** aus.
3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Programmkontrolle:
   - **Sperrung**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert.
   - **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn ein Programm nach Meinung des Benutzers irrtümlich blockiert wurde.
4. Speichern Sie die vorgenommenen Änderungen.

Bewährte Praktiken für die Implementierung einer Liste zulässiger Programme

Bei der Planung der Implementierung einer Liste von erlaubten Programmen wird empfohlen, die folgenden Aktionen durchzuführen:

1. Folgende Typen von Gruppierungen erstellen:
   - Benutzergruppen Gruppen mit Benutzern, für welche die Verwendung unterschiedlicher Sätze von Programmen erlaubt werden soll.
   - Administrationsgruppen Eine oder mehrere Gruppen von Computern, auf die das Kaspersky Security Center die Liste der erlaubten Programme anwendet. Es ist erforderlich, mehrere Gruppen von Computern zu erstellen, wenn für diese Gruppen unterschiedliche Allowlist-Einstellungen verwendet werden.
2. Liste mit Programmen, deren Start erlaubt werden soll, erstellen

Bevor die Liste erstellt wird, sollten die folgenden Aktionen ausgeführt werden:

a. Aufgabe zur Inventarisierung starten

Informationen über die Erstellung, die Einstellungsänderungen und den Start der Inventarisierungsaufgabe sind im Abschnitt „Aufgabenverwaltung“ verfügbar.

b. Liste der ausführbarer Dateien überprüfen

Konfigurieren des Allowlist-Modus für Programme

Um den Allowlist-Modus zu testen, wird folgendes Vorgehen empfohlen:

1. Erstellung von Programmkategorien, die jene Programme enthalten, deren Start erlaubt werden soll

   Sie können eine der folgenden Erstellungsmethoden für die Programmkategorien auswählen:

   - **Manuell zu erweiternde Kategorie**. Sie können diese Kategorie unter Verwendung der folgenden Bedingungen manuell ergänzen:
     - Metadaten einer Datei. Kaspersky Security Center fügt alle ausführbaren Dateien, welche die angegebenen Metadaten aufweisen, zu der Programmkategorie hinzu.
     - Datei-Hash. Kaspersky Security Center fügt alle ausführbaren Dateien, die den angegebenen Hash haben, zu der Programmkategorie hinzu.

       Wenn diese Bedingung verwendet wird, ist die automatische Installation von Updates nicht möglich, da die Dateien der einzelnen Versionen einen unterschiedlichen Hash besitzen.

     - Zertifikat einer Datei. Kaspersky Security Center fügt alle ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind, zu der Programmkategorie hinzu.
     - KL-Kategorie. Kaspersky Security Center nimmt alle ausführbaren Dateien, die zur angegebenen KL-Kategorie gehören, in die Programmkategorie auf.
     - Programmordner. Kaspersky Security Center fügt alle ausführbaren Dateien aus diesem Ordner zu der Programmkategorie hinzu.

       Die Verwendung der Bedingung „Programmordner“ ist riskant, da dann der Start aller Programme aus dem angegebenen Ordner erlaubt wird. Regeln, die Programmkategorien mit der Bedingung „Programmordner“ verwenden, sollten nur für jene Benutzer angewendet werden, für welche die automatische Update-Installation erlaubt werden muss.

   - **Kategorie für ausführbare Dateien aus dem angegebenen Ordner**. Sie können einen Ordner angeben, der ausführbare Dateien enthält, die automatisch in die erstellte Programmkategorie aufgenommen werden sollen.
   - **Kategorie für ausführbare Dateien der gewählten Geräte**. Sie können einen Computer angeben, dessen ausführbare Dateien automatisch in die erstellte Programmkategorie aufgenommen werden sollen.

Wenn Programmkategorien auf diese Weise erstellt werden, erhält Kaspersky Security Center die Informationen über Programme auf dem Computer aus dem Ordner **Ausführbare Dateien**.

2. Wählen Sie den Allowlist-Modus für die Komponente „Programmkontrolle“.

3. Regeln der Programmkontrolle unter Verwendung der erstellten Programmkategorien erstellen

Die Regeln **Goldene Kategorie** und **Vertrauenswürdige Programme mit Update-Funktionen** werden anfänglich für den Zulässigkeitslistenmodus definiert. Diese Regeln der Programmkontrolle entsprechen den KL-Kategorien. Zur KL-Kategorie „Goldene Kategorie“ gehören jene Programme, welche die normale Funktion des Betriebssystems gewährleisten. Zur KL-Kategorie „Vertrauenswürdige Programme mit Update-Funktionen“ gehören Programme mit Update-Funktionen der gängigen Softwarehersteller. Diese Regeln können nicht gelöscht werden. Die Einstellungen dieser Regeln können nicht geändert werden. Standardmäßig ist die Regel **Goldene Kategorie** aktiviert, und die Regel **Vertrauenswürdige Programme mit Update-Funktionen** ist deaktiviert. Der Start von Programmen, welche den Auslösebedingungen dieser Regeln entsprechen, ist für alle Benutzer erlaubt.

Goldene Kategorie

4. Programme festlegen, für welche die automatische Update-Installation erlaubt werden muss

   Sie können die automatische Installation von Updates auf folgende Weise erlauben:

   - Erstellen einer erweiterten Liste mit erlaubten Programmen, nachdem der Start für alle Programme aus beliebigen KL-Kategorien erlaubt wurde

   - Erstellen einer erweiterten Liste mit erlaubten Programmen, nachdem der Start für alle Programme erlaubt wurde, die mit einem Zertifikat signiert sind

     Um den Start alle Programme die mit einem Zertifikat signiert sind, zu erlauben, können Sie eine Kategorie mit einer Bedingung erstellen, die auf einem Zertifikat basiert und in welcher nur der Parameter **Subjekt** mit dem Wert * verwendet wird.

   - Für die Regel der Programmkontrolle den Parameter **Vertrauenswürdige Programme mit Update-Funktionen** festlegen. Ist das Kontrollkästchen aktiviert, so betrachtet Kaspersky Endpoint Security die Programme, welche unter die Regel fallen, als vertrauenswürdige Programme mit Update-Funktionen. Kaspersky Endpoint Security erlaubt den Start von Programmen, die durch in der Regel enthaltene Programme installiert oder aktualisiert wurden, vorausgesetzt, dass auf diese Programme keine Sperrregeln angewendet werden.

     Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.

   - Einen Ordner erstellen und die ausführbaren Dateien jener Programme, für welche Sie die automatische Update-Installation erlauben möchten, in diesen Ordner verschieben. Anschließend eine Programmkategorie mit der Bedingung „Programmordner“ erstellen und den Pfad dieses Ordners angeben. Danach eine Erlaubnisregel erstellen und diese Kategorie auswählen.

     Die Verwendung der Bedingung „Programmordner“ ist riskant, da dann der Start aller Programme aus dem angegebenen Ordner erlaubt wird. Regeln, die Programmkategorien mit der Bedingung „Programmordner“ verwenden, sollten nur für jene Benutzer angewendet werden, für welche die automatische Update-Installation erlaubt werden muss.

Testen des Allowlist-Modus

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Test für Regeln der Programmkontrolle zu aktivieren und ihre Funktion zu analysieren. Wenn der Testlauf aktiviert ist, werden Programme, für welche der Start durch Regeln der Programmkontrolle verboten ist, von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Um den Allowlist-Modus zu testen, wird folgendes Vorgehen empfohlen:

1. Testzeitraum festlegen (von mehreren Tagen bis zu zwei Monaten)
2. Test für die Regeln der Programmkontrolle aktivieren
3. Analyse der Testergebnisse unter Verwendung von Ereignissen aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle" und der Berichte über im Testmodus verbotene Programme
4. Ändern Sie Einstellungen für den Allowlist-Modus unter Berücksichtigung der Analyseergebnisse.

   Aufgrund der Testergebnisse können Sie ausführbare Dateien, die mit Ereignissen zusammenhängen, zu der Programmkategorie hinzufügen.

Unterstützung für den Allowlist-Modus

Nachdem eine Sperraktion der Programmkontrolle ausgewählt wurde, sollte die Unterstützung des Allowlist-Modus fortgesetzt werden. Dazu dient folgendes Vorgehen:

- Funktionsanalyse der Regeln der Programmkontrolle unter Verwendung von Ereignissen aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle" und der Berichte über verbotene Starts
- Analyse von Benutzeranfragen für den Zugriff auf Programme.
- Analysieren Sie unbekannte ausführbare Dateien, indem Sie ihren Ruf im Kaspersky Security Network überprüfen.
- Vor der Installation von Updates für das Betriebssystem oder für Programme, sollten diese Updates in der Testgruppe für Computer installiert werden, um zu überprüfen, wie sie von den Regeln der Programmkontrolle verarbeitet werden.
- Hinzufügen der erforderlichen Programme zu den Kategorien, die in den Regeln der Programmkontrolle verwendet werden

Kontrolle von Netzwerkports

Während der Ausführung von Kaspersky Endpoint Security überwachen die Komponenten Web-Kontrolle, Schutz vor E-Mail-Bedrohungen und Schutz vor Web-Bedrohungen die Datenströme, die über bestimmte Protokolle und bestimmte offene TCP- und UDP-Ports des Benutzercomputers übertragen werden. Die Komponente „Schutz vor E-Mail-Bedrohungen" analysiert beispielsweise die Informationen, die per SMTP-Protokoll übertragen werden, während die Komponente „Schutz vor Web-Bedrohungen" die per HTTP- und FTP-Protokolle übertragenen Informationen analysiert.

Kaspersky Endpoint Security teilt die TCP- und UDP-Ports des Benutzercomputers je nach Angriffswahrscheinlichkeit in mehrere Gruppen ein. Einige Netzwerkports sind für gefährdete Dienste reserviert. Es wird empfohlen, die Netzwerkports, die für anfällige Dienste reserviert sind, genauer zu überwachen, da für sie ein erhöhtes Risiko besteht, Ziel eines Netzwerkangriffs zu werden. Wenn Sie außergewöhnliche Dienste verwenden, denen außergewöhnliche Netzwerkports zugewiesen sind, so können diese Netzwerkports angreifenden Computern ebenfalls als Ziel dienen. Sie können eine Liste von Netzwerkanschlüssen und eine Liste von Programmen angeben, die Netzwerkzugriff anfordern. Diese Ports und Programme erhalten dann bei der Überwachung des Netzwerkverkehrs besondere Aufmerksamkeit von den Komponenten Schutz vor E-Mail-Bedrohungen und Schutz vor Web-Bedrohungen.

Kontrolle aller Netzwerkports aktivieren

Gehen Sie folgendermaßen vor, um die Kontrolle aller Netzwerkports zu aktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Alle Netzwerkports kontrollieren** aus.
4. Speichern Sie die vorgenommenen Änderungen.

Liste der zu kontrollierenden Netzwerkports erstellen

Gehen Sie folgendermaßen vor, um eine Liste der zu kontrollierenden Netzwerkports zu erstellen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Netzwerkports kontrollieren** aus.
4. Klicken Sie auf **Auswählen**.

   Dies öffnet eine Liste von Netzwerkports, die normalerweise für die Übertragung von E-Mail und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.
5. Verwenden Sie den Schalter in der Spalte **Status**, um die Kontrolle von Netzwerkports zu aktivieren oder zu deaktivieren.
6. Gehen Sie folgendermaßen vor, um einen Netzwerkport zur Liste der Netzwerkports hinzuzufügen:
   a. Klicken Sie auf **Hinzufügen**.
   b. Geben Sie in dem sich öffnenden Fenster die Netzwerkportnummer und eine kurze Beschreibung ein.
   c. Setzen Sie den Status **Aktiv** oder **Inaktiv** für die Kontrolle von Netzwerkports.
7. Speichern Sie die vorgenommenen Änderungen.

Wenn der passive FTP-Modus verwendet wird, kann die Verbindung über einen beliebigen Netzwerkport hergestellt werden, der nicht auf der Liste der kontrollierten Ports steht. Um solche Verbindungen zu schützen, aktivieren Sie die Kontrolle aller Netzwerkports oder konfigurieren Sie die Kontrolle der Netzwerkports für Programme, die FTP-Verbindungen herstellen.

Liste der Programme erstellen, für die alle Netzwerkports überwacht werden

Sie können eine Liste mit Programmen erstellen, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll.

Es wird empfohlen, in die Liste der Programme, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll, jene Programme aufzunehmen, die Daten über das FTP-Protokoll empfangen oder senden.

Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Netzwerkports kontrolliert werden sollen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Netzwerkeinstellungen** aus.
3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Netzwerkports kontrollieren** aus.
4. Aktivieren Sie das Kontrollkästchen **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen**.

   Wenn dieses Kontrollkästchen aktiviert ist, kontrolliert Kaspersky Endpoint Security alle Ports für die folgenden Programme:

   - Adobe Reader
   - Apple Application Support
   - Google Chrome
   - Microsoft Edge
   - Mozilla Firefox
   - Internet Explorer
   - Java
   - mIRC
   - Opera
   - Pidgin
   - Safari
   - Mail.ru-Agent

- Yandex.Browser

5. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.

6. Klicken Sie auf **Auswählen**.

   Dies öffnet eine Liste von Programmen, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden.

7. Verwenden Sie den Schalter in der Spalte **Status**, um die Kontrolle von Netzwerkports zu aktivieren oder zu deaktivieren.

8. Wenn ein Programm nicht auf der Programmliste steht, können Sie es wie folgt hinzufügen:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie in dem sich öffnenden Fenster den Pfad zu der ausführbaren Datei des Programms und eine kurze Beschreibung ein.

   c. Setzen Sie den Status **Aktiv** oder **Inaktiv** für die Kontrolle von Netzwerkports.

9. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Listen überwachter Ports

Kaspersky Endpoint Security verwendet die folgenden Listen zur Überwachung von Netzwerkports: Liste der Netzwerkports und Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden. Sie können Listen überwachter Ports in eine XML-Datei exportieren. Anschließend können Sie die Datei ändern, um beispielsweise eine große Anzahl von Ports mit derselben Beschreibung hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um die Listen der überwachten Ports zu sichern oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren von Listen überwachter Ports in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
6. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Netzwerkports kontrollieren** aus.
7. Klicken Sie auf **Einstellungen**.

   Das Fenster **Netzwerkports** wird geöffnet. Im Fenster **Netzwerkports** befindet sich eine Liste der Netzwerkports, die normalerweise für die Übertragung von E-Mails und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.
8. So exportieren Sie die Liste der Netzwerkports:
   a. Wählen Sie in der Liste der Netzwerkports die Ports aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keinen Port ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ports.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der Netzwerkports exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Netzwerkports in die XLM-Datei.
9. So exportieren Sie die Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden:
   a. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.
   b. Wählen Sie in der Liste der Programme die Programme aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie kein Programm ausgewählt haben, exportiert Kaspersky Endpoint Security alle Programme.
   c. Klicken Sie auf **Export**.
   d. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Programme exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   e. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Programme in die XLM-Datei.
10. So importieren Sie die Liste der Netzwerkports:

a. Klicken Sie in der Liste der Netzwerkports auf die Schaltfläche **Import**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Netzwerkports importieren möchten.

b. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Netzwerkports gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

11. So importieren Sie eine Liste von Programmen, deren Ports von Kaspersky Endpoint Security überwacht werden:

a. Klicken Sie in der Liste der Programme auf **Import**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Programme importieren möchten.

b. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Programmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

12. Speichern Sie die vorgenommenen Änderungen.

[Exportieren und Importieren von Listen überwachter Ports in die Web Console und Cloud Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste der überwachten Ports exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Allgemeine Einstellungen → Netzwerkeinstellungen**.
5. So exportieren Sie die Liste der Netzwerkports:

   a. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Netzwerkports kontrollieren** aus.

   b. Klicken Sie auf den Link **n Ports ausgewählt**.

   Das Fenster **Netzwerkports** wird geöffnet. Im Fenster **Netzwerkports** befindet sich eine Liste der Netzwerkports, die normalerweise für die Übertragung von E-Mails und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.

   c. Wählen Sie in der Liste der Netzwerkports die Ports aus, die Sie exportieren möchten.

   d. Klicken Sie auf **Export**.

   e. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der Netzwerkports exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   f. Klicken Sie auf **Speichern**.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Netzwerkports in die XLM-Datei.
6. So exportieren Sie die Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden:

   a. Aktivieren Sie im Block **Überwachte Ports** das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.

   b. Klicken Sie auf den Link **n Programme ausgewählt**.

   c. Wählen Sie in der Liste der Programme die Programme aus, die Sie exportieren möchten.

   d. Klicken Sie auf **Export**.

   e. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Programme exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   f. Klicken Sie auf **Speichern**.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Programme in die XLM-Datei.
7. So importieren Sie die Liste der Netzwerkports:

   a. Klicken Sie in der Liste der Netzwerkports auf die Schaltfläche **Import**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Netzwerkports importieren möchten.

b. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Netzwerkports gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

8. So importieren Sie eine Liste von Programmen, deren Ports von Kaspersky Endpoint Security überwacht werden:

a. Klicken Sie in der Liste der Programme auf **Import**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Programme importieren möchten.

b. Klicken Sie auf **Öffnen**.

Wenn es auf dem Computer bereits eine Liste mit Programmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

9. Speichern Sie die vorgenommenen Änderungen.

Managed Detection and Response

Die Komponente „Managed Detection and Response“ wurde in Version 11.6.0 zu Kaspersky Endpoint Security hinzugefügt. Diese Komponente erleichtert die Interaktion mit der Lösung, die als "Kaspersky Managed Detection and Response" bekannt ist. *Kaspersky Managed Detection and Response (MDR)* sucht, erkennt und eliminiert kontinuierlich Bedrohungen, die gegen Ihr Unternehmen gerichtet sind. Ausführliche Informationen zur Funktionsweise der Lösung *finden Sie in der Hilfe zu Kaspersky Managed Detection and Response*.

Bei der Interaktion mit Kaspersky Managed Detection and Response können Sie mithilfe des Programms die folgenden Funktionen ausführen:

- „Managed Detection and Response“ mithilfe einer BLOB-Konfigurationsdatei aktivieren
- Befehle von Kaspersky Managed Detection and Response ausführen
- Telemetriedaten zur Erkennung von Bedrohungen an Kaspersky Managed Detection and Response senden

Integration mit Kaspersky Managed Detection and Response

Zur Integration von Kaspersky Managed Detection and Response sind folgende Schritte erforderlich:

1. **Private Kaspersky Security Network konfigurieren**

   Überspringen Sie diesen Schritt, wenn Sie „Kaspersky Security Center Cloud Console“ verwenden. „Kaspersky Security Center Cloud Console“ konfiguriert „Local Kaspersky Security Network“ automatisch, wenn das MDR-Plug-in installiert wird.

   Private KSN unterstützt den Datenaustausch zwischen Computern und dedizierten Servern von Kaspersky Security Network, jedoch nicht mit Global KSN.

   Laden Sie in den Eigenschaften des Administrationsservers die Konfigurationsdatei von Kaspersky Security Network hoch. Die Konfigurationsdatei von Kaspersky Security Network befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv in der Konsole von Kaspersky Managed Detection and Response abrufen. Ausführliche Informationen über die Konfiguration von Private KSN finden Sie in der *Hilfe zu Kaspersky Security Center*. Die Konfigurationsdatei von Kaspersky Security Network kann auch über die Befehlszeile auf den Computer hochgeladen werden (siehe Anleitung unten).

   So konfigurieren Sie Private KSN über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   ```
   avp.com KSN /private <Dateiname>
   ```

   `<Dateiname>` ist der Name der Konfigurationsdatei, welche die Einstellungen für Private KSN enthält (Dateiformat „pkcs7“ oder „pem“).

   Beispiel:

   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Als Ergebnis verwendet Kaspersky Endpoint Security Private KSN, um die Reputation von Dateien, Programmen und Websites zu ermitteln. In den Richtlinieneinstellungen im Abschnitt **Kaspersky Security Network** wird der Betriebsstatus *KSN-Netzwerk: Private KSN* angezeigt.

Sie müssen den erweiterten KSN-Modus aktivieren, damit „Managed Detection and Response“ funktioniert.

2 Aktivieren Sie „Managed Detection and Response“.

Laden Sie die BLOB-Konfigurationsdatei in die Richtlinie von Kaspersky Endpoint Security (siehe Anleitung unten). Die BLOB-Datei enthält die Client-ID und Informationen zur Lizenz für Kaspersky Managed Detection and Response. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv in der Konsole von Kaspersky Managed Detection and Response abrufen. Ausführliche Informationen zur BLOB-Datei *finden Sie in der Hilfe zu Kaspersky Managed Detection and Response*.

So aktivieren Sie „Managed Detection and Response“ in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Erweiterter Bedrohungsschutz** → **Detection and Response** aus.
6. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response**.
7. Klicken Sie im Block **Einstellungen** auf **Import** und wählen Sie die BLOB-Datei aus, die in der Konsole von Kaspersky Managed Detection and Response empfangen wurde. Die Datei hat die Erweiterung p7.
8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie „Managed Detection and Response“ in der „Web Console“ und „Cloud Console“

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Erweiterter Bedrohungsschutz** → **Detection and Response** aus.
5. Aktivieren Sie den Schalter **Managed Detection and Response**.
6. Klicken Sie auf **Import** und wählen Sie die BLOB-Datei aus, die über die Konsole von Kaspersky Managed Detection and Response abgerufen wurde. Die Datei hat die Erweiterung p7.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie „Managed Detection and Response“ über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:
   - Wenn die Programmeinstellungen nicht kennwortgeschützt sind:
     `avp.com MDRLICENSE /ADD <Dateiname>`
     `<Dateiname>` ist der Name der BLOB-Konfigurationsdatei zur Aktivierung von Managed Detection and Response (Dateiformat p7).
   - Wenn die Programmeinstellungen kennwortgeschützt sind:
     `avp.com MDRLICENSE /ADD <Dateiname> /login=<Benutzername> /password=<Kennwort>`

Daraufhin verifiziert Kaspersky Endpoint Security die BLOB-Datei. Zur Verifizierung der BLOB-Datei gehört auch die Überprüfung der digitalen Signatur und der Gültigkeitsdauer der Lizenz. Wenn die BLOB-Datei erfolgreich verifiziert wurde, lädt Kaspersky Endpoint Security die Datei hoch und sendet sie bei der nächsten Synchronisierung mit Kaspersky Security Center an den Computer. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Sie können sich den Betriebsstatus einer Komponente auch in den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security ansehen. Die Komponente **Managed Detection and Response** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Sie müssen die folgenden Komponenten aktivieren, damit „Managed Detection and Response“ funktioniert:

- Kaspersky Security Network (erweiterter Modus).
- Verhaltensanalyse.

Das Aktivieren dieser Komponenten ist obligatorisch. Andernfalls funktioniert „Kaspersky Managed Detection and Response“ nicht, da die erforderlichen Telemetriedaten nicht empfangen werden.

„Kaspersky Managed Detection and Response“ verwendet zusätzlich Daten, die von anderen Anwendungen stammen. Das Aktivieren dieser Komponenten ist optional. Diese Komponenten stellen zusätzliche Daten bereit:

- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- Firewall.

Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows

Kaspersky Endpoint Security Version 11 und höher unterstützt die MDR-Lösung. Kaspersky Endpoint Security der Versionen 11 – 11.5.0 sendet nur Telemetriedaten an „Kaspersky Managed Detection and Response“, um die Bedrohungserkennung zu ermöglichen. Kaspersky Endpoint Security Version 11.6.0 umfasst die gesamte Funktionalität des integrierten Agenten (Kaspersky Endpoint Agent).

Wenn Sie Kaspersky Endpoint Security 11 – 11.5.0 verwenden, müssen Sie die Datenbanken auf die neueste Version aktualisieren, um mit der MDR-Lösung arbeiten zu können. Sie müssen auch Kaspersky Endpoint Agent installieren.

Wenn Sie Kaspersky Endpoint Security 11.6.0 oder höher verwenden, müssen Sie bei der Anwendungsinstallation die Komponente „Managed Detection and Response“ auswählen, um mit der MDR-Lösung arbeiten zu können. In diesem Fall müssen Sie Kaspersky Endpoint Agent nicht installieren.

Um von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows zu migrieren:

1. Konfigurieren Sie die Integration von „Kaspersky Managed Detection and Response“ in der Kaspersky Endpoint Security-Richtlinie.
2. Deaktivieren Sie die Komponente „Managed Detection and Response“ in der Kaspersky Endpoint Agent-Richtlinie.

Falls die Kaspersky Endpoint Security-Richtlinie auch für Computer gilt, auf denen Kaspersky Endpoint Security 11 – 11.5.0 nicht installiert ist, müssen Sie zuerst eine separate Kaspersky Endpoint Agent-Richtlinie für diese Computer erstellen. Konfigurieren Sie in der neuen Richtlinie die Integration mit „Kaspersky Managed Detection and Response“.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent gewährleistet die Interaktion zwischen dem Programm und anderen Kaspersky-Lösungen für die Erkennung komplexer Bedrohungen (z. B. Kaspersky Sandbox). Die Kaspersky-Lösungen, die Kaspersky Endpoint Agent unterstützen, sind von der Version von Kaspersky Endpoint Agent abhängig.

Ausführliche Informationen über Kaspersky Endpoint Agent für Windows, das Teil der von Ihnen verwendeten Softwarelösung ist, sowie umfassende Informationen zur Standalone-Lösung finden Sie in der Hilfe zum jeweiligen Produkt:

- *Hilfe zu Kaspersky Anti Targeted Attack Platform*
- *Hilfe zu Kaspersky Sandbox*
- *Hilfe zu Kaspersky Endpoint Detection and Response Optimum*

- *Hilfe zu Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent gehört zum Lieferumfang von Kaspersky Endpoint Security. Sie können Kaspersky Endpoint Agent bei der Installation von Kaspersky Endpoint Security installieren. Dazu müssen Sie bei der Programminstallation die Komponente „Endpoint Agent“ auswählen (z. B. im Installationspaket). Nachdem das Programm mit der Komponente „Endpoint Agent“ installiert wurde, werden Kaspersky Endpoint Security und Kaspersky Endpoint Agent zur Liste der installierten Programme hinzugefügt. Nach der Deinstallation von Kaspersky Endpoint Security wird auch das Programm Kaspersky Endpoint Agent automatisch entfernt.

Daten löschen

Kaspersky Endpoint Security kann die Daten auf Benutzercomputern mithilfe einer Aufgabe ferngesteuert löschen.

Kaspersky Endpoint Security löscht die Daten wie folgt:

- im unbeaufsichtigten Modus.
- auf Festplatten und Wechseldatenträgern.
- für alle Benutzerkonten auf dem Computer.

Kaspersky Endpoint Security führt die Aufgabe *Daten löschen* für einen beliebigen Lizenzierungstyp aus, selbst nach Ablauf der Lizenz.

Modi für die Datenlöschung

Diese Aufgabe bietet die folgenden Modi zur Datenlöschung:

- Sofortige Datenlöschung.

  In diesem Modus können Sie beispielsweise veraltete Daten löschen, um Speicherplatz freizugeben.

- Aufgeschobene Datenlöschung.

  Dieser Modus dient beispielsweise zum Schutz von Daten auf einem Notebook bei Verlust oder Diebstahl. Sie können festlegen, dass die Daten automatisch gelöscht werden, wenn das Notebook das Unternehmensnetzwerk verlässt und längere Zeit nicht mehr mit Kaspersky Security Center synchronisiert wird.

Es ist nicht möglich, einen Zeitplan für die Datenlöschung in den Aufgabeneigenschaften anzupassen. Die Daten können entweder sofort nach dem Aufgabenstart manuell gelöscht werden oder die aufgeschobene Datenlöschung kann festgelegt werden, falls keine Verbindung zu Kaspersky Security Center besteht.

Beschränkungen

Die Datenlöschung besitzt die folgenden Beschränkungen:

- Die Verwaltung der Aufgabe *Daten löschen* steht nur dem Administrator von Kaspersky Security Center zur Verfügung. Die Aufgabe kann auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht angepasst oder gestartet werden.
- Für das NTFS-Dateisystem löscht Kaspersky Endpoint Security nur die Namen der grundlegenden Datenströme. Die Namen alternativer Datenströme können nicht gelöscht werden.
- Wenn Kaspersky Endpoint Security eine symbolische Verknüpfungsdatei löscht, werden auch die Dateien gelöscht, deren Pfade in der symbolischen Verknüpfung angegeben sind.

Erstellung einer Aufgabe zur Datenlöschung

Um die Daten auf Benutzercomputern zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Daten löschen** aus.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Daten löschen (Diebstahlschutz)`.

   d. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

   Wenn zur Administrationsgruppe, für welche die Aufgabe gilt, neue Computer hinzugefügt wurden, wird die Aufgabe zur sofortigen Datenlöschung auf den neuen Computern nur unter der Bedingung gestartet, dass zwischen dem Abschluss der Aufgabenausführung und dem Hinzufügen der neuen Computer weniger als 5 Minuten lagen.

5. Beenden Sie den Assistenten durch Klick auf **Fertig**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die folgende Aufgabe von Kaspersky Endpoint Security: **Daten löschen**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

8. Wählen Sie eine Methode für die Datenlöschung aus:

   - **Mit Betriebssystemmitteln löschen**. Kaspersky Endpoint Security löscht die Dateien mithilfe von Betriebssystemmitteln und verschiebt die Dateien nicht in den Papierkorb.

   - **Endgültig löschen**. Kaspersky Endpoint Security überschreibt die Dateien mit zufälligen Daten. Nach der Löschung ist es praktisch unmöglich, die Daten wiederherzustellen.

9. Wenn Sie die aufgeschobene Datenlöschung verwenden möchten, aktivieren Sie das Kontrollkästchen **Daten automatisch löschen, wenn keine Verbindung zu Kaspersky Security Center besteht länger als n Tage**. Legen Sie die Anzahl der Tage fest.

   Die Aufgabe zur aufgeschobenen Datenlöschung wird jedes Mal ausgeführt, wenn der Zeitraum für das Fehlen einer Verbindung mit Kaspersky Security Center überschritten wird.

Wenn Sie die aufgeschobene Datenlöschung anpassen, berücksichtigen Sie, dass Mitarbeiter ihre Computer beispielsweise während des Urlaubs für längere Zeit ausschalten können. In diesem Fall kann der zulässige Zeitraum für das Fehlen einer Verbindung überschritten werden und die Daten werden gelöscht. Berücksichtigen Sie auch den Zeitplan für die Arbeit von mobilen Mitarbeitern. Details über die Verwendung von Offline-Computern und Offline-Benutzern *finden Sie in der Hilfe für Kaspersky Security Center*.

Ist das Kontrollkästchen deaktiviert, so wird die Aufgabe sofort nach der Synchronisierung mit Kaspersky Security Center ausgeführt.

10. Erstellen Sie eine Liste der zu löschenden Objekte:

    - **Ordner**. Kaspersky Endpoint Security löscht alle Dateien in dem Ordner und in den Unterordnern. Bei der Eingabe des Ordnerpfads unterstützt Kaspersky Endpoint Security keine Masken und Umgebungsvariablen.
    - **Dateien nach Erweiterung**. Kaspersky Endpoint Security führt eine Suche nach Dateien mit den angegebenen Erweiterungen auf allen Computerlaufwerken aus, dazu gehören auch Wechseldatenträger. Um mehrere Erweiterungen hinzuzufügen, verwenden Sie das Zeichen "`;`" oder "`,`".
    - **Standardordner**. Kaspersky Endpoint Security löscht die Dateien aus den folgenden Bereichen:
        - **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner.
        - **Cookies-Dateien**. Dateien, in denen der Browser die Daten von Websites speichert, die der Benutzer besucht hat (z. B. Daten für die Benutzerautorisierung).
        - **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner.
        - **Temporäre Dateien für Internet Explorer**. Temporäre Dateien, die mit der Nutzung des Browsers Internet Explorer zusammenhängen: Kopien von Webseiten, Bilder und Mediendateien.
        - **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Sicherungskopien von Dokumenten.
        - **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB).
        - **Benutzerprofil**. Auswahl von Dateien und Ordnern, in denen Betriebssystemeinstellungen für ein lokales Benutzerkonto gespeichert sind.

    Sie können auf jeder Registerkarte eine Liste der zu löschenden Objekte erstellen. Kaspersky Endpoint Security erstellt eine allgemeine konsolidierte Liste und löscht im Rahmen der Aufgabe die Dateien aus dieser Liste.

    > Dateien, welche für die Funktion von Kaspersky Endpoint Security erforderlich sind, können nicht gelöscht werden.

11. Klicken Sie auf **Speichern**.
12. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
13. Klicken Sie auf **Starten**.

Dadurch werden die Daten auf den Benutzercomputern im ausgewählten Modus gelöscht: sofort oder bei fehlender Verbindung. Kann Kaspersky Endpoint Security eine Datei nicht löschen, da sie beispielsweise gerade vom Benutzer verwendet wird, so versucht das Programm nicht, die Datei erneut zu löschen. Um die Datenlöschung abzuschließen, starten Sie die Aufgabe erneut.

Kennwortschutz

Es kann sein, dass ein Computer von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern sich unterscheiden. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky Endpoint Security und dessen Einstellungen kann das Sicherheitsniveau des Computers insgesamt beeinträchtigen. Mit dem Kennwortschutz können Sie den Benutzerzugriff auf Kaspersky Endpoint Security gemäß den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Beenden des Programms).

Wenn ein Benutzer, der die Windows-Sitzung gestartet hat (*Sitzungsbenutzer*), zur Ausführung von Aktionen berechtigt ist, fragt Kaspersky Endpoint Security nicht nach Benutzername und Kennwort oder temporärem Kennwort. Der Benutzer erhält Zugriff auf Kaspersky Endpoint Security gemäß den vorhandenen Berechtigungen.

Wenn der Sitzungsbenutzer nicht zur Ausführung von Aktionen berechtigt ist, kann der Benutzer wie folgt Zugriff auf das Programm erhalten:

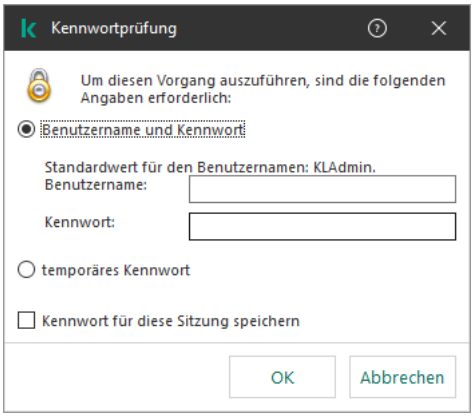
- Benutzername und Kennwort eingeben.

  Diese Methode eignet sich für den regulären Einsatz. Um eine kennwortgeschützte Aktion auszuführen, müssen die Daten eines Domänen-Benutzerkontos mit den erforderlichen Berechtigungen eingegeben werden. Dabei muss sich der Computer in einer Domäne befinden. Wenn sich der Computer nicht in einer Domäne befindet, können Sie das Benutzerkonto KLAdmin verwenden.

- Temporäres Kennwort eingeben.

  Diese Methode ist geeignet, wenn sich ein Benutzer außerhalb des Unternehmensnetzwerks befindet und ihm eine temporäre Berechtigung gewährt werden soll, um eine verbotene Aktion auszuführen (z. B. Programm beenden). Nach Ablauf des temporären Kennworts oder nach dem Ende der Sitzung setzt das Programm die Einstellungen von Kaspersky Endpoint Security in den vorherigen Zustand zurück.

Wenn der Benutzer versucht, eine kennwortgeschützte Aktion auszuführen, fordert Kaspersky Endpoint Security den Benutzer auf, einen Benutzernamen und ein Kennwort oder ein temporäres Kennwort einzugeben (siehe Bild unten).



Kennwortabfrage für den Zugriff auf Kaspersky Endpoint Security

Benutzername und Kennwort

Um auf Kaspersky Endpoint Security zuzugreifen, müssen Sie die Daten des Domänenkontos eingeben. Der Kennwortschutz unterstützt die Verwendung der folgenden Benutzerkonten:

- **KLAdmin**. Administratorkonto ohne Beschränkungen für den Zugriff auf Kaspersky Endpoint Security. Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen. Die Berechtigung für das KLAdmin-Benutzerkonto kann nicht widerrufen werden. Wenn Sie den Kennwortschutz aktivieren, fordert Kaspersky Endpoint Security Sie auf, ein Kennwort für das KLAdmin-Benutzerkonto festzulegen.

- **Gruppe „Alle"**. Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält. Die Benutzer aus der Gruppe „Alle" können gemäß den gewährten Berechtigungen auf das Programm zugreifen.

- **Bestimmte Benutzer oder Gruppen**. Benutzerkonten, für die Sie bestimmte Berechtigungen anpassen können. Wenn beispielsweise eine Aktion für die Gruppe „Alle" verboten ist, können Sie die Aktion für einen bestimmten Benutzer oder eine Gruppe erlauben.

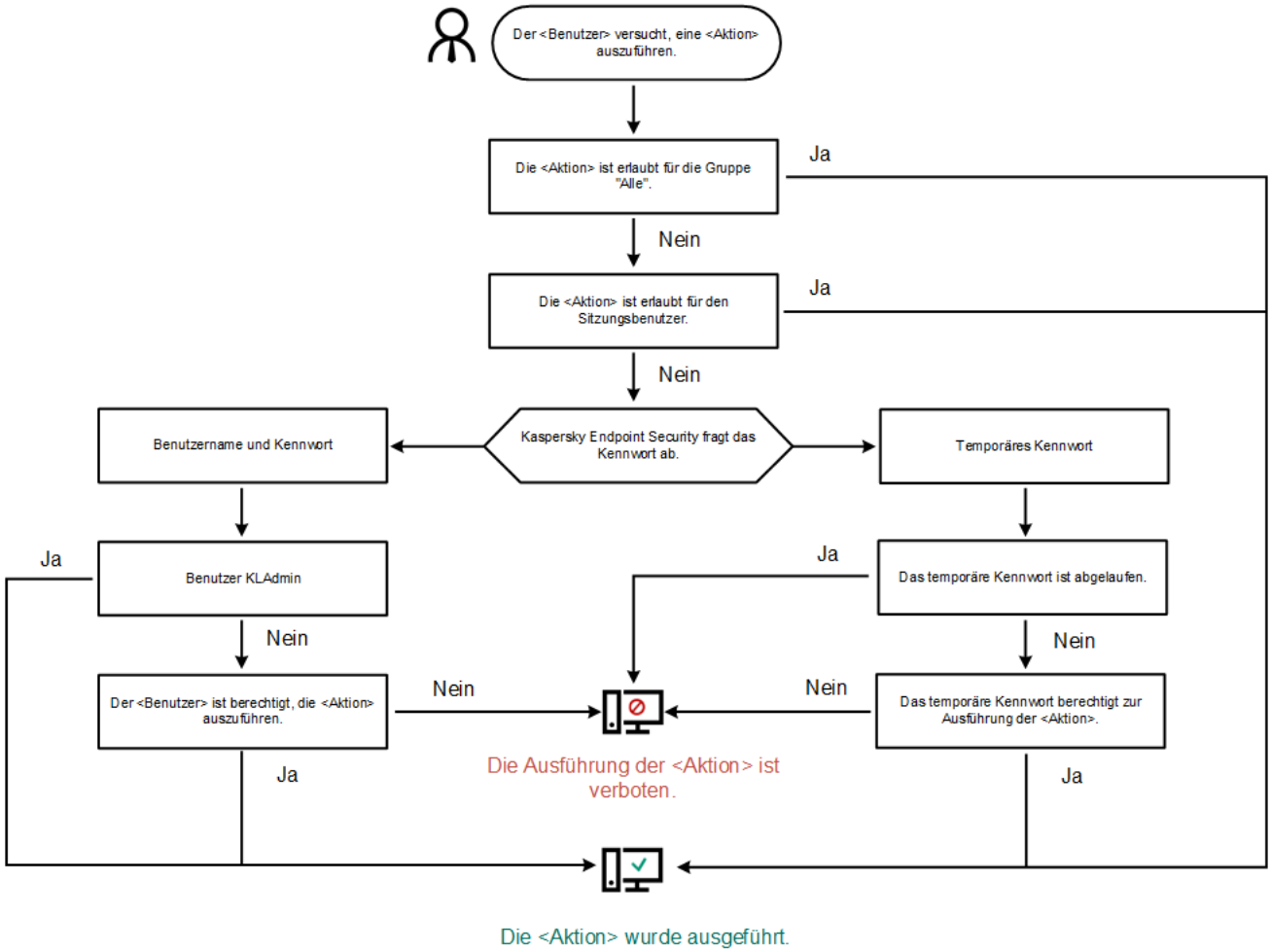
- **Sitzungsbenutzer**. Benutzerkonto, unter dem die Windows-Sitzung gestartet wurde. Sie können den Sitzungsbenutzer während der Kennworteingabe ändern (Kontrollkästchen **Kennwort für diese Sitzung speichern**). In diesem Fall weist Kaspersky Endpoint Security anstelle des Benutzers, der die Windows-Sitzung gestartet hat, den Sitzungsbenutzer zu, dessen Anmeldedaten Sie eingegeben haben.

Temporäres Kennwort

Mit dem temporären Kennwort können Sie für einen einzelnen Computer außerhalb des Unternehmensnetzwerks den temporären Zugriff auf Kaspersky Endpoint Security gewähren. Der Administrator erstellt in Kaspersky Security Center in den Eigenschaften des Benutzercomputers ein temporäres Kennwort für einen bestimmten Computer. Der Administrator wählt die Aktionen aus, für die das temporäre Kennwort gilt, und die Gültigkeitsdauer des temporären Kennworts.

Algorithmus des Kennwortschutzes

Um über die Ausführung einer kennwortgeschützten Aktion zu entscheiden, folgt Kaspersky Endpoint Security dem folgenden Algorithmus (siehe Bild unten).



Algorithmus des Kennwortschutzes

Kennwortschutz aktivieren

Mit dem Kennwortschutz können Sie den Benutzerzugriff auf Kaspersky Endpoint Security gemäß den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Beenden des Programms).

Um den Kennwortschutz zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

   Wählen Sie im Fenster „Einstellungen“ den Abschnitt **Benutzeroberfläche**.

2. Verwenden Sie den Schalter **Kennwortschutz**, um die Komponente zu aktivieren oder zu deaktivieren.

3. Legen Sie ein Kennwort für das KLAdmin-Benutzerkonto fest und bestätigen Sie es.

   Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen.

   Wenn der Computer einer Richtlinie unterliegt, kann der Administrator das Kennwort für das KLAdmin-Benutzerkonto in den Richtlinieneigenschaften zurücksetzen. Wenn der Computer nicht mit Kaspersky Security Center verbunden ist und Sie das Kennwort für das KLAdmin-Benutzerkonto vergessen haben, kann das Kennwort nicht wiederhergestellt werden.

4. Passen Sie Berechtigungen für alle Benutzer im Unternehmensnetzwerk an:

   a. Klicken Sie in der Tabelle **Berechtigungen** auf die Schaltfläche **Bearbeiten**, um die Liste der Berechtigungen für die Gruppe „Jeder“ zu öffnen.

      Die *Gruppe „Alle”* ist die Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält.

   b. Aktivieren Sie die Kontrollkästchen für die Aktionen, die Benutzern ohne Kennworteingabe zur Verfügung stehen sollen.

      Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

      Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

   c. Klicken Sie auf **OK**.

5. Speichern Sie die vorgenommenen Änderungen.

Nach der Aktivierung des Kennwortschutzes beschränkt das Programm den Zugriff der Benutzer auf Kaspersky Endpoint Security gemäß den Berechtigungen für die Gruppe „Alle“. Aktionen, die für die Gruppe „Alle“ verboten sind, können Sie nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts ausführen.

Sie können den Kennwortschutz nur mithilfe des Benutzerkontos KLAdmin deaktivieren. Der Kennwortschutz kann nicht mithilfe eines anderen Benutzerkontos oder mithilfe eines temporären Kennworts deaktiviert werden.

Während der Kennwortprüfung können Sie das Kontrollkästchen **Kennwort für diese Sitzung speichern** aktivieren. In diesem Fall fordert Kaspersky Endpoint Security keine Kennworteingabe, wenn der Benutzer versucht, während der Sitzung eine andere kennwortgeschützte zulässige Aktion auszuführen.

Berechtigungen für bestimmte Benutzer oder Gruppen gewähren

Sie können für bestimmte Benutzer oder Gruppen den Zugriff auf Kaspersky Endpoint Security gewähren. Wenn beispielsweise die Gruppe „Alle“ das Programm nicht beenden darf, können Sie einem bestimmten Benutzer die Berechtigung **Programm beenden** erteilen. In diesem Fall können Sie das Programm nur mithilfe des Kontos dieses Benutzers oder mit dem KLAdmin-Benutzerkonto beenden.

Daten eines Benutzerkontos können nur dann für den Zugriff auf ein Programm verwendet werden, wenn sich der Computer in einer Domäne befindet. Wenn sich der Computer nicht in einer Domäne befindet, können Sie das Benutzerkonto KLAdmin oder ein temporäres Kennwort verwenden.

Um eine Berechtigung für bestimmte Benutzer oder Gruppen zu gewähren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

   Wählen Sie im Fenster „Einstellungen“ den Abschnitt **Benutzeroberfläche**.

2. Klicken Sie in der Tabelle **Kennwortschutz** auf die Schaltfläche **Hinzufügen**.

3. Klicken Sie im geöffneten Fenster auf die Schaltfläche **Benutzer auswählen**.

   Das Windows-Standardfenster zur Auswahl von Benutzern oder Gruppen wird geöffnet.

4. Wählen Sie einen Benutzer oder eine Gruppe in Active Directory aus und bestätigen Sie Ihre Auswahl.

5. Aktivieren Sie in der Liste **Berechtigungen** die Kontrollkästchen für jene Aktionen, die dem hinzugefügten Benutzer oder der Gruppe ohne Kennworteingabe zur Verfügung stehen sollen.

   Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

   Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

6. Speichern Sie die vorgenommenen Änderungen.

Wenn der Zugriff auf das Programm für die Gruppe „Alle“ beschränkt ist, können die Benutzer gemäß den Berechtigungen für diese Benutzer auf Kaspersky Endpoint Security zugreifen.

Verwenden eines temporären Kennworts, um Berechtigungen zu gewähren

Mit dem temporären Kennwort können Sie für einen einzelnen Computer außerhalb des Unternehmensnetzwerks den temporären Zugriff auf Kaspersky Endpoint Security gewähren. Dies ist erforderlich, um die Ausführung einer verbotenen Aktion zu erlauben, ohne dem Benutzer die KLAdmin-Anmeldedaten zu übergeben. Um ein temporäres Kennwort zu verwenden, muss der Computer in Kaspersky Security Center hinzugefügt werden.

Um einem Benutzer mithilfe eines temporären Kennworts die Berechtigung zur Ausführung einer verbotenen Aktion zu gewähren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Programme** aus.
6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
7. Wählen Sie im Fenster mit den Programmeinstellungen den Punkt **Allgemeine Einstellungen → Benutzeroberfläche** aus.
8. Klicken Sie im Abschnitt **Kennwortschutz** auf **Einstellungen**.

   Das Fenster **Kennwortschutz** wird geöffnet.
9. Klicken Sie im Block **Temporäres Kennwort** auf **Einstellungen**.

   Das Fenster **Temporäres Kennwort erstellen** wird geöffnet.
10. Legen Sie im Feld **Ablaufdatum** die Gültigkeitsdauer für das temporäre Kennwort fest.
11. Aktivieren Sie in der Tabelle **Gültigkeitsbereich des temporären Kennworts** die Kontrollkästchen für jene Vorgänge, auf welche der Benutzer nach der Eingabe des temporären Kennworts zugreifen kann.
12. Klicken Sie auf **Erstellen**.

    Ein Fenster mit einem temporären Kennwort wird geöffnet (siehe Bild unten).
13. Kopieren Sie das Kennwort und übergeben Sie es an den Benutzer.

Temporäres Kennwort

Besonderheiten der Berechtigungen für den Kennwortschutz

Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten und Beschränkungen.

Programmeinstellungen anpassen

Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).

Programm beenden

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Schutzkomponenten deaktivieren

- Es ist nicht möglich, für die Gruppe „Alle“ das Deaktivieren von Schutzkomponenten zu erlauben. Um das Deaktivieren von Schutzkomponenten nicht nur dem Benutzer KLAdmin, sondern auch anderen Benutzern zu erlauben, fügen Sie den Benutzer oder die Gruppe mit der Berechtigung **Schutzkomponenten deaktivieren** in den Einstellungen des „Kennwortschutzes“ hinzu.
- Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).
- Um die Schutzkomponenten in den Programmeinstellungen zu deaktivieren, muss der Benutzer über die Berechtigung **Programmeinstellungen anpassen** verfügen.
- Zum Deaktivieren von Schutzkomponenten über das Kontextmenü (mit dem Menüpunkt **Schutz anhalten**) muss ein Benutzer neben der Berechtigung **Kontrollkomponenten deaktivieren** auch die Berechtigung **Schutzkomponenten deaktivieren** haben.

Kontrollkomponenten deaktivieren

- Es ist nicht möglich, für die Gruppe „Alle“ das Deaktivieren von Kontrollkomponenten zu erlauben. Um das Deaktivieren von Schutzkomponenten nicht nur dem Benutzer KLAdmin, sondern auch anderen Benutzern zu erlauben, fügen Sie den Benutzer oder die Gruppe mit der Berechtigung **Kontrollkomponenten deaktivieren** in den Einstellungen des „Kennwortschutzes“ hinzu.
- Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).
- Um die Kontrollkomponenten in den Programmeinstellungen zu deaktivieren, muss der Benutzer über die Berechtigung **Programmeinstellungen anpassen** verfügen.
- Zum Deaktivieren von Kontrollkomponenten über das Kontextmenü (mit dem Menüpunkt **Schutz anhalten**) muss ein Benutzer neben der Berechtigung **Schutzkomponenten deaktivieren** auch die Berechtigung **Kontrollkomponenten deaktivieren** haben.

Richtlinie für Kaspersky Security Center deaktivieren

Eine Deaktivierung der Richtlinie von Kaspersky Security Center für die Gruppe „Alle“ kann nicht erlaubt werden. Um die Deaktivierung der Richtlinie nicht nur dem Benutzer KLAdmin, sondern auch anderen Benutzern zu erlauben, fügen Sie den Benutzer oder die Gruppe mit der Berechtigung **Richtlinie für Kaspersky Security Center deaktivieren** in den Einstellungen für den „Kennwortschutz“ hinzu.

Schlüssel löschen

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Programm entfernen / ändern / reparieren

Wenn Sie das Entfernen, Ändern und Wiederherstellen des Programms für die Gruppe „Alle“ erlaubt haben, fordert Kaspersky Endpoint Security kein Kennwort an, wenn der Benutzer versucht, diese Aktionen auszuführen. Daher kann jeder Benutzer, auch Benutzer von außerhalb der Domäne, die Anwendung installieren, ändern oder wiederherstellen.

Zugriffswiederherstellung für Daten auf verschlüsselten Geräten

Sie können den Zugriff auf die Daten auf verschlüsselten Geräten nur mithilfe des KLAdmin-Benutzerkontos wiederherstellen. Es ist nicht möglich, diese Aktion einem anderen Benutzer zu erlauben.

Berichte anzeigen

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Wiederherstellung aus dem Backup

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Vertrauenswürdige Zone

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt.

Die vertrauenswürdige Zone wird manuell vom Systemadministrator angelegt. Berücksichtigt werden dabei die Besonderheiten von Objekten, die für die Arbeit erforderlich sind, sowie die Programme, die auf dem Computer installiert sind. Die Aufnahme von Objekten und Programmen in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Endpoint Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt oder Programm unschädlich ist. Ein Administrator kann einem Benutzer auch erlauben, seine eigene lokale vertrauenswürdige Zone für einen bestimmten Computer zu erstellen. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen.

Erstellung von Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme.

Die Untersuchungsausnahmen ermöglichen es, mit legalen Programmen zu arbeiten, die von Angreifern für eine Beschädigung des Computers oder der Benutzerdaten verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Angreifern verwendet werden. Nähere Informationen zu legalen Programmen, die von Angreifern missbraucht werden können, um den Computer oder die Daten des Anwenders zu beschädigen, erhalten Sie auf der Website der Viren-Enzyklopädie von Kaspersky.

Derartige Programme können bei der Ausführung von Kaspersky Endpoint Security gesperrt werden. Sie können Untersuchungsausnahmen anpassen, um eine Sperrung von notwendigen Programmen zu verhindern. Dazu muss der vertrauenswürdigen Zone der Name oder eine Namensmaske hinzugefügt werden, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht. Es kann beispielsweise sein, dass Sie häufig mit dem Programm Radmin, zur Remote-Administration von Computern. Eine solche Programmaktivität wird von Kaspersky Endpoint Security als schädlich eingestuft und kann blockiert werden. Um zu verhindern, dass ein Programm gesperrt wird, muss eine Untersuchungsausnahme erstellt werden. In dieser Ausnahme wird ein Name oder eine Namensmaske angegeben, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht.

Ein auf Ihrem Computer installiertes Programm, das Informationen sammelt und zur Verarbeitung weiterleitet, kann von Kaspersky Endpoint Security als schädlich eingestuft werden. Um dies zu vermeiden, können Sie das Programm von der Untersuchung ausschließen. Dazu können Sie Kaspersky Endpoint Security entsprechend anpassen, wie in dieser Dokumentation beschrieben.

Untersuchungsausnahmen können von folgenden Komponenten und Programmaufgaben verwendet werden, die vom Systemadministrator erstellt wurden:

- Verhaltensanalyse.
- Exploit-Prävention.
- Programm-Überwachung.
- Schutz vor bedrohlichen Dateien.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.

- Untersuchungsaufgaben.

Ein Objekt wird nicht von Kaspersky Endpoint Security untersucht, wenn beim Start einer Untersuchungsaufgabe das Laufwerk, auf dem sich das Objekt befindet, oder der Ordner, in dem sich das Objekt befindet, zum Untersuchungsbereich gehört. Wenn jedoch beim Start einer benutzerdefinierten Untersuchungsaufgabe dieses Objekt ausdrücklich ausgewählt wird, so bleibt die Untersuchungsausnahme unberücksichtigt.

So erstellen Sie eine Untersuchungsausnahme in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen** aus.
6. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf **Einstellungen**.
7. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Untersuchungsausnahmen**.

   Dies öffnet ein Fenster mit einer Liste der Ausnahmen.
8. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.
9. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen zulassen**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten Dateien weiterhin von Untersuchungen aus.
10. Klicken Sie auf **Hinzufügen**.
11. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

    a. Aktivieren Sie unter **Eigenschaften** das Kontrollkästchen **Datei oder Ordner**.

    b. Öffnen Sie mit dem Link **Datei oder Ordner wählen**, der sich im Block **Beschreibung der Untersuchungsausnahme** befindet, das Fenster **Datei- oder Ordnername**.

    c. Geben Sie entweder den Datei- oder Ordnernamen oder die Maske eines Datei- oder Ordnernamens ein, oder klicken Sie auf **Durchsuchen** und wählen Sie in der Ordnerstruktur eine Datei oder einen Ordner aus.

    Verwenden Sie Masken:

    - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.

- Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt im Ordner `Folder` und in den Unterordnern. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.

- Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

d. Klicken Sie im Fenster **Datei- oder Ordnername** auf **OK**.

Im Fenster **Untersuchungsausnahme** erscheint im Abschnitt **Beschreibung der Untersuchungsausnahme** ein Link für die hinzugefügte Datei oder den Ordner.

12. Um Objekte mit einem bestimmten Namen von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

a. Aktivieren Sie im Abschnitt **Eigenschaften** das Kontrollkästchen **Objektname**.

b. Öffnen Sie mit dem Link **Objektnamen eingeben**, der sich im Abschnitt **Beschreibung der Untersuchungsausnahme** befindet, das Fenster **Objektname**.

c. Um den Namen des Objekttyps einzugeben, verwenden Sie die Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

d. Klicken Sie im Fenster **Objektname** auf **OK**.

Im Fenster **Untersuchungsausnahme** erscheint unter **Beschreibung der Untersuchungsausnahme** ein Link für den hinzugefügten Objektnamen.

13. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten:

a. Aktivieren Sie im Abschnitt **Eigenschaften** das Kontrollkästchen **Objekthash**.

b. Klicken Sie auf den Link zum Objekthash-Eintrag, damit das Fenster **Hash des Objekts** geöffnet wird.

c. Geben Sie den Dateihash ein oder wählen Sie die Datei durch Klicken auf die Schaltfläche **Durchsuchen** aus.

Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

d. Klicken Sie im Fenster **Objekthash** auf **OK**.

Im Fenster **Untersuchungsausnahme** erscheint unter **Beschreibung der Untersuchungsausnahme** ein Link für das hinzugefügte Objekt.

14. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

15. Legen Sie die Komponenten von Kaspersky Endpoint Security fest, für die eine Untersuchungsausnahme verwendet werden soll.

a. Aktivieren Sie mit dem Link **alle** im Abschnitt **Beschreibung der Untersuchungsausnahme** den Link **Komponenten wählen**.

b. Öffnen Sie mit dem Link **Komponenten wählen** das Fenster **Schutzkomponenten**.

c. Aktivieren Sie die Kontrollkästchen für jene Komponenten, für welche die Untersuchungsausnahme gelten soll.

d. Klicken Sie im Fenster **Schutzkomponenten** auf **OK**.

Sind Komponenten in den Einstellungen einer Untersuchungsausnahme angegeben, so gilt die Ausnahme nur für diese Komponenten von Kaspersky Endpoint Security.

Sind keine Komponenten in den Einstellungen einer Untersuchungsausnahme angegeben, so gilt die Ausnahme für alle Komponenten von Kaspersky Endpoint Security.

16. Über das Kontrollkästchen können Sie eine Ausnahme jederzeit stoppen.

17. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Untersuchungsausnahme in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie eine Ausnahme hinzufügen möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Wählen Sie **Allgemeine Einstellungen → Ausnahmen** aus.

5. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf den Link **Untersuchungsausnahmen**.

6. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.

7. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen zulassen**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten Dateien weiterhin von Untersuchungen aus.

8. Klicken Sie auf **Hinzufügen**.

9. Wählen Sie aus, wie Sie die Ausnahme hinzufügen möchten: **Datei oder Ordner**, **Objektname** oder **Hash des Objekts**.

10. Wenn Sie eine Datei oder einen Ordner von Untersuchungen ausschließen möchten, wählen Sie die Datei oder den Ordner aus, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

    Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen * und ? bei der Eingabe einer Maske:

    - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.

    - Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt im Ordner `Folder` und in den Unterordnern. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.

    - Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske

`C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

11. Wenn Sie einen bestimmten Objekttyp von Untersuchungen ausschließen möchten, geben Sie im Feld **Objekt** den Namen des Objekttyps gemäß der Klassifizierung der Kaspersky-Enzyklopädie ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

    Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

12. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten, geben Sie den Dateihash im Feld **Datei-Hash** ein.

    Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

13. Wählen Sie im Block **Schutzkomponenten** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

14. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

15. Über den Schalter können Sie eine Ausnahme jederzeit stoppen.

16. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Untersuchungsausnahme in der Programmoberfläche

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wenn Sie eine Datei oder einen Ordner von Untersuchungen ausschließen möchten, wählen Sie die Datei oder den Ordner aus, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

   Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen * und ? bei der Eingabe einer Maske:

   - Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.
   - Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt im Ordner `Folder` und in den Unterordnern. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.
   - Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.
6. Wenn Sie einen bestimmten Objekttyp von Untersuchungen ausschließen möchten, geben Sie im Feld **Objekt** den Namen des Objekttyps gemäß der Klassifizierung der Kaspersky-Enzyklopädie ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

   Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.
7. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten, geben Sie den Dateihash im Feld **Datei-Hash** ein.

   Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.
8. Wählen Sie im Block **Schutzkomponenten** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.
9. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.
10. Wählen Sie den Status **Aktiv** für die Ausnahme.

    Über den Schalter können Sie eine Ausnahme jederzeit stoppen.
11. Speichern Sie die vorgenommenen Änderungen.

Beispiele für Pfadmasken:
Pfade für Dateien, die sich in einem beliebigen Ordner befinden können:

- Die Maske `*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe.
- Die Maske `Beispiel*` umfasst alle Pfade von Dateien mit dem Namen BEISPIEL.

Pfade für Dateien, die sich in einem bestimmten Ordner befinden können:

- Die Maske `C:\dir\*.*` umfasst alle Pfade von Dateien im Ordner C:\dir\, allerdings nicht in den untergeordneten Ordnern von C:\dir\.
- Die Maske `C:\dir\*` umfasst alle Pfade von Dateien im Ordner C:\dir\, allerdings nicht in den untergeordneten Ordnern von C:\dir\.
- Die Maske `C:\dir\` umfasst alle Pfade von Dateien im Ordner C:\dir\, allerdings nicht in den untergeordneten Ordnern von C:\dir\.
- Die Maske `C:\dir\*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe im Ordner C:\dir\, allerdings nicht in den untergeordneten Ordnern von C:\dir\.
- Die Maske `C:\dir\test` umfasst alle Pfade von Dateien mit dem Namen test im Ordner C:\dir\, allerdings nicht in den untergeordneten Ordnern von C:\dir\.
- Die Maske `C:\dir\*\test` umfasst alle Pfade von Dateien mit dem Namen test im Ordner C:\dir\ und in den untergeordneten Ordnern von C:\dir\.

Pfade für Dateien, die sich in allen Ordnern mit dem angegebenen Namen befinden können:

- Die Maske `dir\*.*` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\*` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\test` umfasst alle Pfade von Dateien mit dem Namen test in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieses Ordners.

Aktivierung und Deaktivierung von Untersuchungsausnahmen

Gehen Sie wie folgt vor, um die Anwendung einer Untersuchungsausnahme zu starten oder zu beenden:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.

3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

4. Wählen Sie die entsprechende Ausnahme aus der Liste der Untersuchungsausnahmen aus.

5. Verwenden Sie den Schalter neben einem Objekt, um dieses Objekt in den Untersuchungsbereich aufzunehmen oder ihn davon auszuschließen.

6. Speichern Sie die vorgenommenen Änderungen.

Liste mit vertrauenswürdigen Programmen erstellen

Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Endpoint Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme sowie den von ihnen erzeugten Netzwerkverkehr. Ein Programm, das zur Liste der vertrauenswürdigen Programme hinzugefügt wurde, wird von Kaspersky Endpoint Security allerdings aus der Untersuchung ausgeschlossen.

Wenn Sie beispielsweise die Objekte, die von dem Microsoft-Windows-Programm Editor verwendet werden, für ungefährlich und eine Untersuchung dieser Objekte für nicht erforderlich halten, so vertrauen Sie diesem Programm und sollten das Programm Editor zur Liste der vertrauenswürdigen Programme hinzufügen. Beim Untersuchen werden dann Objekte übersprungen, die von diesem Programm verwendet werden.

Außerdem können spezielle Aktionen, die von Kaspersky Endpoint Security als schädlich klassifiziert werden, im Rahmen bestimmter Programme ungefährlich sein. So ist das Abfangen eines Textes, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (z. B. Punto Switcher) ein normaler Vorgang. Es wird empfohlen, solche Programme in die Liste der vertrauenswürdigen Programme aufzunehmen, um ihre speziellen Funktionen zu berücksichtigen und sie von der Aktivitätskontrolle auszuschließen.

Wenn vertrauenswürdige Programme von der Untersuchung ausgeschlossen werden, lassen sich Kompatibilitätsprobleme von Kaspersky Endpoint Security mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Endpoint Security und durch ein anderes Antiviren-Programm). Außerdem wird dadurch die Leistung des Computers erhöht, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms werden jedoch weiterhin auf Viren und andere Schadprogramme untersucht. Verwenden Sie Untersuchungsausnahmen, um ein Programm vollständig aus der Untersuchung durch Kaspersky Endpoint Security auszuschließen.

So fügen Sie ein Programm zur vertrauenswürdigen Liste in der Verwaltungskonsole (MMC) hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen** aus.
6. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf **Einstellungen**.
7. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Vertrauenswürdige Programme**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.
8. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der vertrauenswürdigen Programme für alle Computer des Unternehmens erstellen möchten. Die Listen mit vertrauenswürdigen Programmen der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Programme der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Programme der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.
9. Aktivieren Sie das Kontrollkästchen **Verwendung lokal vertrauenswürdiger Programme erlauben**, wenn Sie dem Benutzer die Erstellung einer lokalen Liste vertrauenswürdiger Programme ermöglichen möchten. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Liste vertrauenswürdiger Programme eine eigene lokale Liste vertrauenswürdiger Programme erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten vertrauenswürdigen Programme zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten vertrauenswürdigen Programme weiterhin von Untersuchungen aus.
10. Klicken Sie auf **Hinzufügen**.
11. Geben Sie im geöffneten Fenster den Pfad zur ausführbaren Datei des vertrauenswürdigen Programms ein.

    Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

    > Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn eine Liste mit vertrauenswürdigen Programmen in der Kaspersky Security Center-Konsole erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen * verwenden (z. B. `C:\Users\*\Documents\File.exe`).

    > Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.
12. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

13. Mit dem Kontrollkästchen können Sie ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen.

14. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie ein Programm zur vertrauenswürdigen Liste in der Web-Konsole und der Cloud-Konsole hinzu

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie das Programm zur Liste der vertrauenswürdigen Programme hinzufügen möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Allgemeine Einstellungen → Ausnahmen** aus.
5. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf den Link **Vertrauenswürdige Programme**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.
6. Aktivieren Sie das Kontrollkästchen **Werte bei Vererbung zusammenfassen**, wenn Sie eine konsolidierte Liste der vertrauenswürdigen Programme für alle Computer des Unternehmens erstellen möchten. Die Listen mit vertrauenswürdigen Programmen der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Programme der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Programme der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.
7. Aktivieren Sie das Kontrollkästchen **Verwendung lokal vertrauenswürdiger Programme erlauben**, wenn Sie dem Benutzer die Erstellung einer lokalen Liste vertrauenswürdiger Programme ermöglichen möchten. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Liste vertrauenswürdiger Programme eine eigene lokale Liste vertrauenswürdiger Programme erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten vertrauenswürdigen Programme zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security nach Deaktivierung dieser Funktion die aufgelisteten vertrauenswürdigen Programme weiterhin von Untersuchungen aus.
8. Klicken Sie auf **Hinzufügen**.
9. Geben Sie im geöffneten Fenster den Pfad zur ausführbaren Datei des vertrauenswürdigen Programms ein.

   Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

   > Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn eine Liste mit vertrauenswürdigen Programmen in der Kaspersky Security Center-Konsole erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen * verwenden (z. B. `C:\Users\*\Documents\File.exe`).

   > Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.
10. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

11. Mit dem Kontrollkästchen können Sie ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen.

12. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie ein Programm in der Programmschnittstelle zur vertrauenswürdigen Liste hinzu

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.

3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.

4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

5. Wählen Sie die ausführbare Datei des vertrauenswürdigen Programms aus.

   Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

   > Kaspersky Endpoint Security unterstützt Umgebungsvariablen und konvertiert den Pfad in der lokalen Programmoberfläche. Mit anderen Worten: Wenn Sie den Dateipfad `%userprofile%\Documents\File.exe` eingeben, wird der Eintrag `C:\Users\Fred123\Documents\File.exe` auf der lokalen Benutzeroberfläche des Programms für den Benutzer Fred123 hinzugefügt. Dementsprechend ignoriert Kaspersky Endpoint Security das vertrauenswürdige Programm `File.exe` für andere Benutzer. Um diesen Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`).

   > Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.

6. Konfigurieren Sie im Fenster „Eigenschaften“ der vertrauenswürdigen Programme die erweiterten Einstellungen (siehe Tabelle unten).

7. Mit dem Schalter können Sie ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen.

8. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für vertrauenswürdige Programme

Einstellung	Beschreibung
Zu öffnende Dateien nicht untersuchen	Alle Dateien, die vom Programm geöffnet werden, sind von der Überprüfung durch Kaspersky Endpoint Security ausgeschlossen. Wenn Sie z. B. Programme zur Sicherung von Dateien verwenden, trägt diese Funktion dazu bei, den Ressourcenverbrauch von Kaspersky Endpoint Security zu reduzieren.
Programmaktivität nicht kontrollieren	Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität des Programms im Betriebssystem nicht. Die Programmaktivität wird durch die folgenden Komponenten überwacht: Verhaltensanalyse, Exploit-Prävention, Programm-Überwachung, Rollback von schädlichen Aktionen und Firewall.
Beschränkungen des	Die für den übergeordneten Prozess konfigurierten Einschränkungen werden von Kaspersky Endpoint Security nicht auf einen untergeordneten Prozess angewendet.

übergeordneten Prozesses (Programms) nicht übernehmen	Der übergeordnete Prozess wird von einem Programm gestartet, für das Programmrechte (Host Intrusion Prevention) und Netzwerkregeln für das Programm (Firewall) konfiguriert sind.
Aktivität der Unterprogramme nicht kontrollieren	Kaspersky Endpoint Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden.
Interaktion mit der Schnittstelle von Kaspersky Endpoint Security ermöglichen	Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security blockiert alle Versuche, Programme von einem Remote-Computer aus zu verwalten. Ist dieses Kontrollkästchen aktiviert, wird einem Remote-Administrationsprogramm erlaubt, Einstellungen für Kaspersky Endpoint Security über die Benutzeroberfläche von Kaspersky Endpoint Security zu verwalten.
Die Interaktion mit der AMSI-Schutzkomponente nicht blockieren *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Kaspersky Endpoint Security überwacht nicht die Anfragen des vertrauenswürdigen Programms nach Objekten, die von der AMSI-Schutzkomponente untersucht werden sollen.
Verschlüsselten Datenverkehr nicht untersuchen / Gesamten Datenverkehr nicht untersuchen	Der von diesem Programm initiierte Netzwerkverkehr wird von den Untersuchungen durch Kaspersky Endpoint Security ausgeschlossen. Sie können entweder den gesamten Verkehr oder nur den verschlüsselten Verkehr von den Untersuchungen ausschließen. Sie können auch einzelne IP-Adressen und Portnummern von Untersuchungen ausschließen.
Kommentar	Falls erforderlich, können Sie einen kurzen Kommentar für das vertrauenswürdige Programm eingeben. Kommentare tragen dazu bei, die Suche und Sortierung von vertrauenswürdigen Programmen zu vereinfachen.
Zustand	Status des vertrauenswürdigen Programms: • **Aktiv** Status bedeutet, dass sich das Programm in der vertrauenswürdigen Zone befindet. • **Inaktiv** Status bedeutet, dass sich das Programm von der vertrauenswürdigen Zone ausgeschlossen ist.

Aktivieren und Deaktivieren von Regeln der vertrauenswürdigen Zone für ein Programm aus der Liste der vertrauenswürdigen Programm

Um Regeln der vertrauenswürdigen Zone für ein Programm aus der Liste der vertrauenswürdigen Programm zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.
4. Wählen Sie in der Liste der vertrauenswürdigen Programme das entsprechende vertrauenswürdige Programm aus.

5. Verwenden Sie den Schalter in der Spalte **Status**, um ein vertrauenswürdiges Programm in den Untersuchungsbereich aufzunehmen oder es davon auszuschließen.

6. Speichern Sie die vorgenommenen Änderungen.

Vertrauenswürdigen Zertifikatspeicher des Systems verwenden

Durch die Verwendung des Zertifikatspeichers des Systems können Programme, die eine vertrauenswürdige digitale Signatur besitzen, von der Untersuchung auf Viren ausgeschlossen werden. Kaspersky Endpoint Security weist solche Programme automatisch der Gruppe *Vertrauenswürdig* zu.

Um mit der Verwendung des vertrauenswürdigen Zertifikatspeichers des Systems zu beginnen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.

3. Wählen Sie in der Dropdown-Liste **Vertrauenswürdiger Zertifikatspeicher des Systems** aus, welchen Systemspeicher Kaspersky Endpoint Security als vertrauenswürdig betrachten soll.

4. Speichern Sie die vorgenommenen Änderungen.

Arbeit mit dem Backup

Das *Backup* ist ein Speicher für Backup-Kopien von Dateien, die bei der Desinfektion verändert oder gelöscht wurden. Eine *Backup-Kopie* ist die Kopie einer Datei, die vor der Desinfektion oder dem Löschen dieser Datei angelegt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Backup-Kopien von Dateien werden im Ordner `C:\ProgramData\Kaspersky Lab\KES\QB` gespeichert.

Vollständige Zugriffsrechte auf diesen Ordner besitzen die Benutzer der Gruppe „Administratoren“. Beschränkte Zugriffsrechte für diesen Ordner besitzt der Benutzer, unter dessen Benutzerkonto die Installation von Kaspersky Endpoint Security ausgeführt wurde.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Es kann vorkommen, dass Dateien bei der Desinfektion nicht vollständig erhalten bleiben. Wenn wichtige Informationen, die in einer Datei enthalten waren, aufgrund einer Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, die Datei aus ihrer Backup-Kopie in den ursprünglichen Ordner der Datei wiederherzustellen.

Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Backup-Kopien für Dateien an den Administrationsserver von Kaspersky Security Center übertragen werden. Details über die Arbeit mit Backup-Kopien für Dateien in Kaspersky Security Center finden Sie im Hilfesystem zu Kaspersky Security Center.

Maximale Speicherdauer für Dateien im Backup anpassen

Die maximale Speicherdauer für Backup-Kopien im Backup beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.

Um eine maximale Speicherdauer für Dateien im Backup festzulegen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Berichte und Speicherung** aus.
3. Wenn Sie die Speicherdauer für Kopien von Dateien im Backup begrenzen möchten, aktivieren Sie das Kontrollkästchen **Objekte speichern für maximal n Tage** im Block **Backup**. Geben Sie im Feld rechts vom Kontrollkästchen **Objekte speichern für maximal n Tage** an, wie lange Dateikopien im Backup maximal aufbewahrt werden sollen.
4. Speichern Sie die vorgenommenen Änderungen.

Maximale Größe für das Backup anpassen

Sie können die maximale Größe des Backups angeben. Die Größe des Backups ist standardmäßig nicht beschränkt. Nach Erreichen der maximalen Größe löscht Kaspersky Endpoint Security automatisch die ältesten Dateien aus dem Backup.

Um die maximale Größe für das Backup anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Berichte und Speicherung** aus.
3. Wenn Sie die Größe des Backups begrenzen möchten, aktivieren Sie das Kontrollkästchen **Begrenzen der Backup-Größe auf n MB** im Block **Backup**. Die maximale Größe des Backups angeben.
4. Speichern Sie die vorgenommenen Änderungen.

Dateien aus dem Backup wiederherstellen

Wird in einer Datei schädlicher Code gefunden, so blockiert Kaspersky Endpoint Security die Datei, weist Ihr den Status *Infiziert* zu, legt im Backup eine Backup-Kopie an und führt einen Desinfektionsversuch aus. War die Desinfektion erfolgreich, ändert sich der Status der Sicherungskopie in *Desinfiziert*. Die Datei ist ursprünglichen Speicherordner wieder verfügbar. Falls die Datei nicht desinfiziert werden kann, wird sie von Kaspersky Endpoint Security aus dem Ursprungsordner gelöscht. Sie können die Datei aus einer desinfizierten Backup-Kopie im ursprünglichen Ordner wiederherstellen.

Dateien mit dem Status *Wird beim Neustart des Computers desinfiziert* können nicht wiederhergestellt werden. Starten Sie den Computer neu. Danach ändert sich der Dateistatus in *Desinfiziert* oder *Gelöscht*. Nun können Sie die Datei aus ihrer Backup-Kopie im ursprünglichen Ordner wiederherstellen.

Wenn schädlicher Code in einer Datei gefunden wird, die zu einer Anwendung aus dem Windows Store gehört, kopiert Kaspersky Endpoint Security die Datei nicht ins Backup, sondern löscht die Datei sofort. Die Integrität einer Anwendung aus dem Windows Store kann mithilfe von Microsoft Windows 8 wiederhergestellt werden (Details über die Wiederherstellung einer Anwendung aus dem Windows Store finden Sie im *Hilfesystem für Microsoft Windows 8*).

Die Backup-Kopien werden in einer Liste angezeigt. Für die Backup-Kopie einer Datei wird der Pfad des Ordners, an dem diese Datei ursprünglich gespeichert war, angezeigt. Der Pfad des ursprünglichen Ordners der Datei kann persönliche Daten enthalten.

Wenn sich in einem Backup-Ordner mehrere Dateien mit identischen Namen und unterschiedlichen Inhalten befinden, so kann nur jene Datei wiederhergestellt werden, die zuletzt ins Backup verschoben wurde.

Gehen Sie folgendermaßen vor, um Dateien aus dem Backup wiederherzustellen:

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Speicher**.

   Das Fenster **Backup** wird geöffnet.
2. Wählen Sie in der Tabelle im Fenster **Backup** eine oder mehrere Backup-Dateien aus.
3. Klicken Sie auf **Wiederherstellen**.

   Kaspersky Endpoint Security stellt die Dateien aus den ausgewählten Backup-Kopien in den ursprünglichen Ordnern wieder her.

Backup-Kopien von Dateien aus dem Backup löschen

Backup-Kopien, deren maximale Speicherdauer verstrichen ist, werden unabhängig von ihrem Status automatisch aus dem Backup gelöscht. Die Speicherdauer ist in den Programmeinstellungen festgelegt. Sie können eine beliebige Kopie einer Datei auch selbst aus dem Backup löschen.

Gehen Sie folgendermaßen vor, um Backup-Kopien aus dem Backup zu löschen:

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Speicher**.

   Das Fenster **Backup** wird geöffnet.

2. Markieren Sie die Sicherungskopien der Dateien, die Sie aus dem Backup löschen möchten, und klicken Sie auf die Schaltfläche **Löschen**. Sie können auch alle Dateien aus dem Backup löschen, indem Sie auf die Schaltfläche **Alle löschen** klicken.

Kaspersky Endpoint Security löscht die gewählten Backup-Kopien aus dem Backup.

Benachrichtigungsdienst

Während der Ausführung von Kaspersky Endpoint Security treten unterschiedliche Ereignisse ein. Benachrichtigungen über diese Ereignisse können rein informativ sein oder wichtige Informationen enthalten. Eine Benachrichtigung kann beispielsweise über das erfolgreiche Update der Datenbanken und Programm-Module informieren oder auf die Funktionsstörung einer bestimmten Komponente hinweisen, die Sie beheben müssen.

Kaspersky Endpoint Security bietet die Möglichkeit, Informationen über Ereignisse, die im Programm eintreten, im Microsoft Windows-Ereignisbericht und/oder im Bericht für Kaspersky Endpoint Security aufzuzeichnen.

Kaspersky Endpoint Security bietet folgende Optionen für die Zustellung von Benachrichtigungen:

- mithilfe von Pop-up-Benachrichtigungen im Infobereich der Microsoft-Windows-Taskleiste
- per E-Mail

Die Benachrichtigungsmethoden können angepasst werden. Die Benachrichtigungsmethode wird für jeden Ereignistyp konfiguriert.

Wenn Sie mit der Ereignistabelle arbeiten, um den Benachrichtigungsdienst anzupassen, können Sie folgende Aktionen ausführen:

- Filtern der Ereignisse des Benachrichtigungsdienstes nach den Spaltenwerten oder anhand eines komplexen Filters
- Verwenden der Suchfunktion für Ereignisse des Benachrichtigungsdienstes
- Sortieren der Ereignisse des Benachrichtigungsdienstes
- Ändern der Reihenfolge und der Auswahl von Spalten, welche in der Ereignisliste des Benachrichtigungsdienstes angezeigt werden

Einstellungen der Ereignisberichte anpassen

Gehen Sie folgendermaßen vor, um die Einstellungen der Ereignisberichte anzupassen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster „Einstellungen“ den Abschnitt **Benutzeroberfläche**.
3. Klicken Sie im Abschnitt **Benachrichtigungen** auf die Schaltfläche **Benachrichtigungen einrichten**.

   Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

   In Ereignissen können die folgenden Benutzerdaten enthalten sein:

   - Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
   - Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden
   - Benutzername für Microsoft Windows

- Adressen von Webseiten, die vom Benutzer geöffnet wurden

4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, deren Ereignisberichte Sie konfigurieren möchten.

5. Aktivieren Sie für die entsprechenden Ereignisse die Kontrollkästchen in den Spalten **In lokalem Bericht speichern** und **Im Windows-Ereignisprotokoll speichern**.

   Ereignisse, für welche das Kontrollkästchen in der Spalte **In lokalem Bericht speichern** aktiviert ist, werden in den **Anwendungs- und Dienstprotokollen** im Abschnitt **Kaspersky Event Log** angezeigt. Ereignisse, für welche das Kontrollkästchen in der Spalte **Im Windows-Ereignisprotokoll speichern** aktiviert ist, werden in **Windows-Protokollen** im Abschnitt **Anwendung** angezeigt. Um die Ereignisprotokolle zu öffnen, wählen Sie **Start** → **Systemsteuerung** → **Verwaltung** → **Ereignisanzeige** aus.

6. Speichern Sie die vorgenommenen Änderungen.

Anzeige und Versand von Benachrichtigungen anpassen

Um die Anzeige und den Versand von Benachrichtigungen anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster „Einstellungen“ den Abschnitt **Benutzeroberfläche**.

3. Klicken Sie im Abschnitt **Benachrichtigungen** auf die Schaltfläche **Benachrichtigungen einrichten**.

   Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

   In Ereignissen können die folgenden Benutzerdaten enthalten sein:

   - Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
   - Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden
   - Benutzername für Microsoft Windows
   - Adressen von Webseiten, die vom Benutzer geöffnet wurden

4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, für die der Versand von Meldungen angepasst werden soll.

5. Aktivieren Sie in der Spalte **Auf dem Bildschirm anzeigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden auf dem Bildschirm im Infobereich der Microsoft-Windows-Taskleiste als Pop-up-Benachrichtigungen angezeigt.

6. Aktivieren Sie in der Spalte **Per E-Mail benachrichtigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden als E-Mail-Nachricht gesendet, wenn die Einstellungen für den Versand von E-Mail-Benachrichtigungen festgelegt sind.

7. Klicken Sie auf **OK**.

8. Wenn Sie E-Mail-Benachrichtigungen aktiviert haben, konfigurieren Sie die Einstellungen für die E-Mail-Zustellung:

    a. Klicken Sie auf **E-Mail-Benachrichtigungen anpassen**.

    b. Aktivieren Sie das Kontrollkästchen **Ereignisse melden**, um den Versand zu aktivieren. Benachrichtigungen erfolgen für in Kaspersky Endpoint Security eingetretene Ereignisse, die in der Spalte **Per E-Mail benachrichtigen** markiert sind.

    c. Passen Sie den Versand von E-Mail-Meldungen an.

    d. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen.

Anzeige von Warnungen über den Programmstatus im Infobereich anpassen

Um die Anzeige von Warnungen über den Programmstatus im Infobereich der Taskleiste anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster „Einstellungen“ den Abschnitt **Benutzeroberfläche**.

3. Aktivieren Sie im Abschnitt **Status des Programms im Benachrichtigungsbereich anzeigen** die Kontrollkästchen für jene Ereigniskategorien, über die im Infobereich der Microsoft-Windows-Taskleiste Benachrichtigungen angezeigt werden sollen.

4. Speichern Sie die vorgenommenen Änderungen.

Treten Ereignisse auf, die zu den ausgewählten Kategorien gehören, so ändert sich das Programmsymbol im Infobereich der Taskleiste je nach Priorität der Warnung in oder .

Arbeit mit Berichten

In den Berichten werden protokolliert: Informationen über Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

Die Berichte werden im Ordner `C:\ProgramData\Kaspersky Lab\KES\Report` gespeichert.

Die Berichte können die folgenden Benutzerdaten enthalten:

- Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
- Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden
- Benutzername für Microsoft Windows
- Adressen von Webseiten, die vom Benutzer geöffnet wurden

Die Daten werden im Bericht als Tabelle angezeigt. Jede Tabellenzeile enthält Informationen zu einem separaten Ereignis. Die Ereignisattribute befinden sich in den Tabellenspalten. Einige Spalten sind nochmals unterteilt und enthalten Unterspalten mit zusätzlichen Attributen. Um zusätzliche Attribute anzuzeigen, klicken Sie auf die Schaltfläche ⊞ neben dem Namen der Spalte. Die Ereignisse, die bei der Ausführung von Komponenten oder bei der Ausführung von Aufgaben registriert werden, besitzen unterschiedliche Attribute.

Folgende Berichte sind verfügbar:

- Bericht **Systemaudit**. Enthält Informationen über Ereignisse, welche bei der Interaktion zwischen Benutzer und Programm eintreten, sowie Ereignisse, welche den generellen Programmbetrieb betreffen und sich nicht auf bestimmte Komponenten oder Aufgaben von Kaspersky Endpoint Security beziehen.
- Berichte über die Komponenten von Kaspersky Endpoint Security.
- Berichte über die Ausführung der Aufgaben von Kaspersky Endpoint Security.
- Bericht für die **Virtuelle Datentresore**. Enthält Informationen über die Ereignisse, welche bei der Verschlüsselung und Entschlüsselung von Daten auftreten.

In Berichten werden folgenden Prioritätsstufen für Ereignisse verwendet:

ⓘ **Informative Ereignisse**. Referenzereignisse mit informativem Charakter, welche in der Regel keine wichtigen Informationen enthalten.

⚠ **Warnungen**. Ereignisse, die beachtet werden müssen, da sie auf wichtige Situationen bei der Ausführung von Kaspersky Endpoint Security hinweisen.

🛑 **Kritische Ereignisse**. Ereignisse mit kritischer Priorität, die auf Probleme bei der Ausführung von Kaspersky Endpoint Security oder auf Schwachstellen im Schutz des Benutzercomputers hinweisen.

Zur Vereinfachung der Arbeit mit Berichten können Sie die Darstellung der Daten auf dem Bildschirm wie folgt ändern:

- Ereignisliste nach verschiedenen Kriterien filtern

- Funktion zur Suche nach einem bestimmten Ereignis verwenden
- Ausgewähltes Ereignis in einem separaten Block anzeigen
- Ereignisliste nach einer bestimmten Spalte des Berichts sortieren
- Ereignisse, die mithilfe eines Filters gruppiert sind, durch Klick auf die Schaltfläche ⊞ anzeigen und ausblenden
- Reihenfolge und Zusammensetzung der im Bericht angezeigten Spalten ändern

Bei Bedarf können Sie den erstellten Bericht in einer Textdatei speichern. Außerdem können Sie Informationen aus den Berichten löschen. Dazu können die Informationen nach den Komponenten und Aufgaben von Kaspersky Endpoint Security gruppiert werden.

Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Informationen über Ereignisse an den Administrationsserver von Kaspersky Security Center übertragen werden (Details finden Sie in der *Hilfe zu Kaspersky Endpoint Security*).

Berichte anzeigen

Ist für einen Benutzer die Anzeige der Berichte verfügbar, so kann dieser Benutzer alle Ereignisse, die in den Berichten vorhanden sind, einsehen.

Um Berichte anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen** → **Berichte**.
2. Wählen Sie im linken Bereich des Fensters **Berichte** in der Liste mit Komponenten und Aufgaben eine Komponente oder eine Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen für die Ausführungsergebnisse der ausgewählten Komponente oder der ausgewählten Aufgabe von Kaspersky Endpoint Security enthält. Die Ereignisse können im Bericht nach den Werten in den Zellen aus einer der Spalten sortiert werden. Standardmäßig sind die Ereignisse im Bericht in aufsteigender Reihenfolge nach den Werten in den Zellen der Spalte **Ereignisdatum** sortiert.
3. Ausführliche Informationen über ein bestimmtes Ereignis finden Sie im Bericht dieses Ereignisses.

   Im unteren Fensterbereich wird ein Abschnitt mit zusammenfassenden Informationen über das Ereignis angezeigt.

Maximale Speicherdauer für Berichte anpassen

Die standardmäßige Speicherdauer für Berichte über die von Kaspersky Endpoint Security protokollierten Ereignisse beträgt 30 Tage. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei.

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Berichte und Speicherung** aus.
3. Wenn Sie die Speicherdauer der Berichte begrenzen möchten, aktivieren Sie das Kontrollkästchen **Berichte speichern für maximal n Tage** im Block **Berichte**. Definieren Sie die maximale Speicherdauer für Berichte.
4. Speichern Sie die vorgenommenen Änderungen.

Maximale Größe der Berichtsdatei anpassen

Sie können für die Datei, die den Bericht enthält, eine maximale Größe festlegen. Die maximale Größe der Berichtsdatei ist standardmäßig auf 1024 MB begrenzt. Nach Erreichen der maximalen Berichtsdateigröße löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.

Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Berichte und Speicherung** aus.
3. Aktivieren Sie im Block **Berichte** das Kontrollkästchen **Maximale Dateigröße n MB**, wenn Sie die Größe einer Berichtsdatei begrenzen möchten. Definieren Sie die maximale Größe der Berichtsdatei.
4. Speichern Sie die vorgenommenen Änderungen.

Bericht in Datei speichern

Der Benutzer ist selbst verantwortlich für die Sicherheit der Informationen, welche aus dem Bericht in einer Datei gespeichert werden, und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf diese Informationen.

Der erstellte Bericht kann im Textformat als txt- oder csv-Datei gespeichert werden.

Kaspersky Endpoint Security speichert das Ereignis im Bericht in der gleichen Form, in welcher das Ereignis auf dem Bildschirm angezeigt wird. Die Zusammensetzung und die Reihenfolge der Ereignisattribute bleiben also unverändert.

Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:

1. Klicken Sie im Programmhauptfenster auf **Weitere Funktionen → Berichte**.
2. Wählen Sie im geöffneten Fenster die Komponente oder Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen über die Ausführung der gewählten Komponente oder Aufgabe von Kaspersky Endpoint Security enthält.
3. Die Darstellung der Berichtsdaten kann bei Bedarf mit folgenden Methoden geändert werden:
   - Ereignisse filtern

- Ereignisse suchen
- Anordnung der Spalten ändern
- Ereignisse sortieren

4. Klicken Sie auf die Schaltfläche **Bericht speichern**, die sich rechts oben im Fenster befindet.
5. Geben Sie in dem sich öffnenden Fenster den Zielordner für die Berichtdatei an.
6. Geben Sie im Feld **Dateiname** einen Namen für die Berichtsdatei an.
7. Wählen Sie im Feld **Dateityp** ein Format für die Berichtsdatei: TXT oder CSV.
8. Speichern Sie die vorgenommenen Änderungen.

Berichte löschen

Gehen Sie folgendermaßen vor, um Informationen aus den Berichten zu löschen.

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Abschnitt **Berichte und Speicherung** aus.
3. Klicken Sie im Block **Berichte** auf die Schaltfläche **Löschen**.
4. Wenn der Kennwortschutz aktiviert ist, kann Kaspersky Endpoint Security Sie zur Eingabe der Anmeldedaten für das Benutzerkonto auffordern. Das Programm fordert zur Eingabe von Kontoanmeldedaten auf, wenn der Benutzer nicht über die erforderlichen Berechtigungen verfügt.

Kaspersky Endpoint Security löscht alle Berichte für alle Programmkomponenten und Aufgaben.

Selbstschutz für Kaspersky Endpoint Security

Kaspersky Endpoint Security schützt den Computer vor Schadsoftware, die versucht, die Funktionen von Kaspersky Endpoint Security zu blockieren oder das Programm vom Computer zu entfernen. Der Umfang der Selbstschutztechnologien für verfügbaren Kaspersky Endpoint Security hängt davon ab, ob das Betriebssystem 32-Bit oder 64-Bit ist (beachten Sie die folgende Tabelle).

Selbstschutztechnologien für Kaspersky Endpoint Security

Technologie	Beschreibung	x86-Computer	x64-Computer
Selbstschutz-Modul	Die Technologie blockiert den Zugriff auf die folgenden Anwendungskomponenten: • Dateien im Installationsorder von Kaspersky Endpoint Security • Registrierungsschlüssel mit Einträgen, die zur Anwendung gehören • Prozesse, die von der Anwendung ausgeführt werden	✓	✓
AM-PPL (Antimalware Protected Process Light)	Die Technologie schützt die Kaspersky Endpoint Security-Prozesse vor schädlichen Aktionen. Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019.	✓	–
Modul für den Schutz vor externer Steuerung	Die Technologie beschränkt die Steuerung von Kaspersky Endpoint Security mithilfe von Fernverwaltungsprogrammen (wie z. B. TeamViewer oder RemotelyAnywhere).	✓	– (außer für Windows 7)

Selbstschutz-Mechanismus aktivieren und deaktivieren

Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security ist standardmäßig aktiviert.

Gehen Sie folgendermaßen vor, um den Selbstschutz-Mechanismus zu aktivieren oder zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Verwenden Sie das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstverteidigungsmechanismus zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Aktivierung und Deaktivierung der AM-PPL-Unterstützung

Kaspersky Endpoint Security unterstützt die Technologie Antimalware Protected Process Light (im Folgenden „AM-PPL“) von Microsoft. AM-PPL schützt die Prozesse von Kaspersky Endpoint Security vor schädlichen Aktionen (z. B. Beenden des Programms). AM-PPL erlaubt nur den Start von vertrauenswürdigen Prozessen. Die Prozesse von Kaspersky Endpoint Security sind gemäß den Anforderungen für die Windows-Sicherheit signiert und sind deshalb vertrauenswürdig. Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Standardmäßig ist die Technologie AM-PPL aktiviert.

Kaspersky Endpoint Security besitzt auch integrierte Schutz-Module für die Programmprozesse. Die AM-PPL-Unterstützung erlaubt es, Funktionen für den Schutz von Prozessen an das Betriebssystem zu delegieren. Dadurch erhöhen Sie die Leistung des Programms und reduzieren den Verbrauch von Computerressourcen.

Der Dienst AM-PPL ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019.

Um die AM-PPL-Unterstützung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Deaktivieren Sie das Modul für den Selbstschutz des Programms.

   Das Selbstschutz-Modul verhindert, dass Programmprozesse im Arbeitsspeicher des Computers verändert und gelöscht werden. Dazu gehört auch eine Änderung des AM-PPL-Status.

2. Starten Sie den Befehlszeileninterpreter cmd als Administrator.

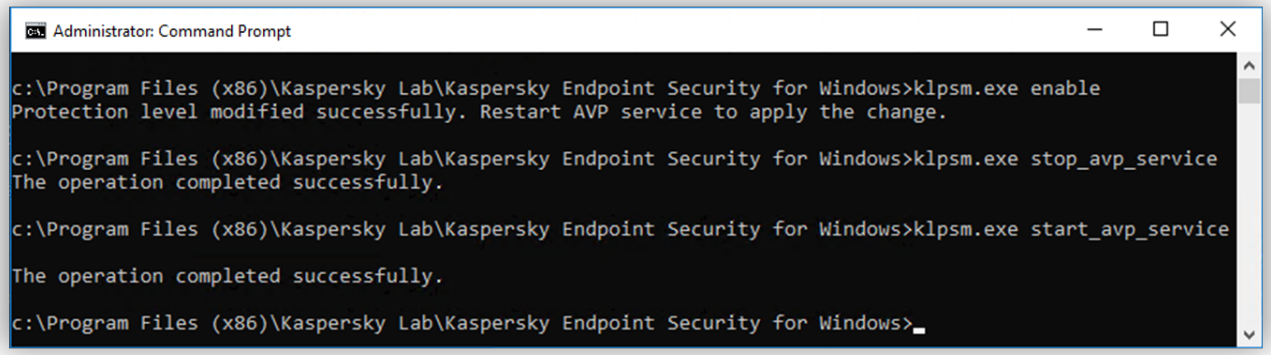
3. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

4. Geben Sie in der Befehlszeile ein:

   - `klpsm.exe enable` – Aktivierung der Unterstützung für die AM-PPL-Technologie (siehe folgende Abb.).
   - `klpsm.exe disable` – Deaktivierung der Unterstützung für die AM-PPL-Technologie.

5. Starten Sie Kaspersky Endpoint Security neu.

6. Setzen Sie das Modul für den Selbstschutz des Programms fort.



Aktivierung der Unterstützung für die AM-PPL-Technologie

Mechanismus zum Schutz vor externer Steuerung aktivieren und deaktivieren

Mit dem Schutz vor externer Steuerung können Sie verbieten, dass Kaspersky Endpoint Security mithilfe von Fernverwaltungsprogrammen (wie z. B. TeamViewer oder RemotelyAnywhere) gesteuert wird. Diese Technologie hat folgende Zwecke:

- Schutz vor Änderungen der Kaspersky Endpoint Security-Einstellungen.
- Schutz vor Steuerung der Dienste von Kaspersky Endpoint Security (wie dem Dienst `AVP`).
- Schutz vor dem Beenden von Anwendungsprozessen.

Der Schutz vor externer Steuerung ist nur für Computer mit 32-Bit-Betriebssystemen verfügbar. Die Technologie ist nicht verfügbar für Computer mit 64-Bit-Betriebssystemen.

So aktivieren oder deaktivieren Sie den Schutz vor externer Verwaltung:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen den Punkt **Erweiterte Einstellungen** → **Allgemein** aus.
3. Verwenden Sie das Kontrollkästchen **Verwaltung der Einstellungen für Kaspersky Endpoint Security über Fernverwaltungsprogramme erlauben**, um den Schutz vor Änderungen der Kaspersky Endpoint Security-Einstellungen zu aktivieren oder zu deaktivieren. Wenn Sie Programme zur Remote-Administration verwenden, sollten Sie die Verwaltung der Einstellungen für Kaspersky Endpoint Security zulassen und die Programme zur Liste der vertrauenswürdigen Programme hinzufügen. Nicht vertrauenswürdige Programme zur Remote-Administration dürfen die Einstellungen von Kaspersky Endpoint Security nicht ändern, auch wenn das Kontrollkästchen **Verwaltung der Einstellungen für Kaspersky Endpoint Security über Fernverwaltungsprogramme erlauben** aktiviert ist. Dieses Kontrollkästchen ist nicht verfügbar, wenn das Kontrollkästchen **Selbstschutz aktivieren** aktiviert ist.
4. Verwenden Sie das Kontrollkästchen **Externe Dienststeuerung aktivieren**, um den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung zu aktivieren oder zu deaktivieren.

   Um das Programm über die Befehlszeile zu beenden, deaktivieren Sie den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung.

5. Speichern Sie die vorgenommenen Änderungen.

Wenn die Mechanismen zum Schutz vor externer Steuerung aktiviert sind, verhindert Kaspersky Endpoint Security daher, dass der Mauszeiger auf das Programmsymbol zeigt. Wenn ein Remote-Benutzer versucht, einen Programmdienst herunterzufahren, erscheint ein Systemfenster mit einer Fehlermeldung.

Gewährleistung der Funktion von Programmen für Remote-Administration

Es kann vorkommen, dass Programme für Remote-Administration eingesetzt werden sollen, während der Schutz vor Fernsteuerung aktiviert ist.

Gehen Sie folgendermaßen vor, um Remote-Administrationsprogramme verwenden zu können:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.
4. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
5. Wählen Sie die ausführbare Datei des Fernverwaltungsprogramms aus.

   Sie können den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
6. Aktivieren Sie das Kontrollkästchen **Programmaktivität nicht kontrollieren**.
7. Speichern Sie die vorgenommenen Änderungen.

Leistung von Kaspersky Endpoint Security und Kompatibilität mit anderen Programmen

Leistung von Kaspersky Endpoint Security

Unter der Leistung von Kaspersky Endpoint Security sind die Anzahl der erkennbaren Objekttypen, die dem Computer Schaden zufügen können, sowie der Energieverbrauch und die benötigten Computerressourcen zu verstehen.

Erkennbare Objekttypen wählen

Kaspersky Endpoint Security erlaubt es, den Computerschutz flexibel anzupassen und die Objekttypen auszuwählen, die das Programm bei seiner Ausführung erkennen soll. Kaspersky Endpoint Security untersucht das Betriebssystem stets auf Viren, Würmer und trojanische Programme. Die Untersuchung dieser Objekttypen kann nicht deaktiviert werden. Diese Programme können dem Computer erheblichen Schaden zufügen. Um das Schutzniveau zu erhöhen, können Sie die Liste der erkennbaren Objekttypen erweitern. Aktivieren Sie dazu die Kontrolle der Aktionen legaler Programme, die von Angreifern zur Beschädigung des Computers und der Benutzerdaten genutzt werden können.

Energiesparmodus nutzen

Bei mobilen Computern ist der Energieverbrauch, der von Programmen verursacht wird, ein wichtiges Thema. Häufig beanspruchen die von Kaspersky Endpoint Security nach Zeitplan ausgeführten Aufgaben erhebliche Ressourcen. Läuft der Computer im Akkubetrieb, können Sie zur Gewährleistung einer längeren Akkulaufzeit den Energiesparmodus nutzen.

Der Energiesparmodus ermöglicht eine automatische Verschiebung von Aufgaben, für die ein Start nach Zeitplan festgelegt ist:

- Update-Aufgabe
- Aufgabe zur vollständigen Untersuchung
- Aufgabe zur Untersuchung wichtiger Bereiche
- Aufgabe zur benutzerdefinierten Untersuchung
- Aufgabe zur Integritätsprüfung

Unabhängig davon, ob der Energiesparmodus aktiviert ist oder nicht, hält Kaspersky Endpoint Security laufende Verschlüsselungsaufgaben an, wenn ein Laptop in den Batteriebetrieb wechselt. Wenn der Laptop aus dem Batteriebetrieb in den Netzbetrieb wechselt, setzt das Programm die Verschlüsselungsaufgaben fort.

Computerressourcen für andere Programme freigeben

Der von Kaspersky Endpoint Security verursachte Verbrauch von Computerressourcen kann sich auf die Leistung anderer Programme auswirken. Um Probleme zu vermeiden, die bei gleichzeitiger Verwendung mit anderen Programmen aufgrund erhöhter Auslastung des Prozessors und der Laufwerksubsysteme auftreten können, kann Kaspersky Endpoint Security die Ausführung geplanter Untersuchungsaufgaben anhalten und Ressourcen für andere Programme freigeben.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Ausführung solcher Programme unabhängig sein soll, sollten ihnen keine Betriebssystemressourcen überlassen werden.

Bei Bedarf können Sie diese Aufgaben auch manuell starten.

Technologie zur Desinfektion aktiver Infektionen nutzen

Moderne schädliche Programme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Bei Erkennen einer schädlichen Aktivität im Betriebssystem nimmt Kaspersky Endpoint Security eine erweiterte Desinfektion vor, wobei eine spezielle Technologie zur Desinfektion aktiver Infektionen zum Einsatz kommt. Die *Technologie zur Desinfektion aktiver Infektionen* dient dazu, schädliche Programme aus dem Betriebssystem zu entfernen, falls diese ihre Prozesse bereits im Arbeitsspeicher gestartet haben und Kaspersky Endpoint Security daran hindern, sie auf reguläre Weise zu neutralisieren. Dadurch wird die Bedrohung neutralisiert. Es wird davon abgeraten, während der aktiven Desinfektion neue Prozesse zu starten oder die Registrierung des Betriebssystems zu ändern. Die Technologie zur Desinfektion aktiver Infektionen beansprucht erhebliche Betriebssystemressourcen, wodurch die Ausführung anderer Programme verlangsamt werden kann.

Nachdem die aktive Desinfektion auf einem Computer mit Microsoft Windows Workstation abgeschlossen wurde, fragt Kaspersky Endpoint Security den Benutzer um Erlaubnis für einen Neustart des Computers. Nach dem Neustart des Computers löscht Kaspersky Endpoint Security die Schadsoftware-Dateien und startet eine vereinfachte vollständige Untersuchung des Computers.

Auf einem Computer mit Microsoft Windows für Server ist eine Abfrage für den Neustart des Computers nicht möglich. Dies ist durch Besonderheiten des Programms Kaspersky Endpoint Security bedingt. Ein ungeplanter Neustart des Dateiservers kann zu Problemen führen. Es kann zu einer vorübergehenden Nichtverfügbarkeit der Dateiserverdaten oder zum Verlust von nicht gespeicherten Daten kommen. Es wird empfohlen, den Neustart eines Dateiservers streng nach Zeitplan auszuführen. Aus diesem Grund ist die Technologie zur aktiven Desinfektion für Dateiserver standardmäßig deaktiviert.

Wird auf einem Dateiserver eine aktive Infektion erkannt, so wird ein Ereignis an Kaspersky Security Center gesendet, das über die Notwendigkeit einer aktiven Desinfektion informiert. Für die aktive Desinfektion eine Infektion, muss auf dem Server die Technologie zur aktiven Desinfektion für Server aktiviert werden und die Gruppenaufgabe *Virensuche* gestartet werden. Dafür sollte ein Zeitpunkt gewählt werden, der für die Benutzer des Servers günstig ist.

Erkennbare Objekttypen wählen

Gehen Sie folgendermaßen vor, um die Typen der erkennbaren Objekte zu wählen:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.
3. Aktivieren Sie im Abschnitt **Arten von erkannten Objekten** die Kontrollkästchen gegenüber den Objekttypen, die Kaspersky Endpoint Security erkennen soll:
   - **Viren, Würmer**

Unterkategorie: Viren und Würmer (Viruses_and_Worms)

Bedrohungsstufe: hoch

Klassische Viren und Würmer führen auf einem Computer Aktionen aus, die nicht vom Benutzer erlaubt wurden. Sie können sich selbst kopieren, wobei die Kopien ebenfalls zur Reproduktion fähig sind.

Klassischer Virus

Nachdem ein klassischer Virus in ein System eingedrungen ist, infiziert er eine Datei, aktiviert sich darin, führt seine schädlichen Aktionen aus und fügt anderen Dateien Kopien von sich hinzu.

Ein klassischer Virus vermehrt sich nur auf lokalen Computerressourcen und kann nicht selbständig in andere Rechner eindringen. Er kann nur auf andere Computer gelangen, wenn er seine Kopie einer Datei hinzufügt, die in einem gemeinsamen Ordner oder auf einer eingelegten CD gespeichert wird, oder wenn der Benutzer eine E-Mail-Nachricht verschickt, an welche die infizierte Datei angehängt ist.

Der Code eines klassischen Virus kann in unterschiedliche Computerbereiche, in das Betriebssystem oder in Programme eindringen. Abhängig vom Milieu werden *Dateiviren*, *Bootviren*, *Skriptviren* und *Makroviren* unterschieden.

Viren verwenden unterschiedliche Methoden, um Dateien zu infizieren. *Überschreibende Viren* (Overwriting) schreiben ihren Code anstelle des Codes einer infizierten Datei und zerstören deren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht repariert werden. *Parasitäre Viren* (Parasitic) verändern Dateien, wobei diese vollständig oder teilweise funktionsfähig bleiben. *Companion-Viren* (Companion) verändern Dateien nicht, sondern legen Zwillingsdateien an. Beim Öffnen einer infizierten Datei wird ihr Zwilling gestartet, der ein Virus ist. Außerdem gibt es noch folgende Virentypen: *Linkviren* (Link), Viren, *die Objektmodule* (OBJ), *Compiler-Bibliotheken* (LIB) oder *den Quelltext von Programmen* infizieren, u.a.

Wurm

Genau wie bei einem klassischen Virus aktiviert sich der Code eines Wurms nach dem Eindringen in ein System selbst und führt seine schädlichen Aktionen aus. Die Bezeichnung Wurm geht darauf zurück, dass er wie ein Wurm von Computer zu Computer „kriechen" und seine Kopien ohne Erlaubnis des Benutzers über verschiedene Datenkanäle verbreiten kann.

Würmer werden grundsätzlich nach der Art ihrer Verbreitung unterschieden. Die folgende Tabelle klassifiziert die Wurmtypen nach der Verbreitungsmethode.

Verbreitungsmethoden von Würmern

Typ	Name	Beschreibung
Email-Worm	Email-Worm	Sie verbreiten sich über E-Mails. Eine infizierte E-Mail-Nachricht enthält eine angehängte Datei mit einer Wurmkopie oder einem Link zu einer solchen Datei, die sich auf einer gehackten oder speziell erstellten Website befindet. Wenn Sie die angehängte Datei öffnen, wird der Wurm aktiviert. Wenn Sie auf den Link klicken, die Datei herunterladen und dann öffnen, beginnt der Wurm auch mit seinen bösartigen Aktionen. Danach verbreitet er seine Kopien. Dazu sucht er andere E-Mail-Adressen und schickt infizierte Nachrichten an diese.
IM-Worm	SMTP-Clients	Sie verbreiten sich über IM-Clients.

		Ein IM-Wurm verschickt in der Regel Nachrichten mit einem Link, der zu einer Website mit seiner Kopie führt, an die Adressen der Kontaktliste. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats. Dies sind Chat-Systeme, mit denen über das Internet in Echtzeit Gespräche mit mehreren Teilnehmern möglich sind. Ein solcher Wurm veröffentlicht im Internet-Chat eine Datei mit seiner Kopie oder einem Link zu einer Datei. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
Net-Worm	Netzwürmer (Würmer für Computernetzwerke)	Sie verbreiten sich über Computernetzwerke. Im Unterschied zu anderen Wurmtypen verbreitet sich ein Netzwurm ohne Zutun des Benutzers. Er sucht im lokalen Netzwerk nach Computern, auf denen Programme laufen, die Schwachstellen aufweisen. Zu diesem Zweck schickt er ein spezielles Netzwerkpaket (Exploit), das den Wurmcode oder einen Teil davon enthält. Befindet sich ein „verwundbarer" Computer im Netzwerk, nimmt er das Netzwerkpaket an. Nachdem der Wurm vollständig in den Computer eingedrungen ist, aktiviert er sich.
P2P-Worm	Würmer für Dateitausch-Netzwerke	Sie verbreiten sich über Peer-to-Peer-Netze. Um in ein P2P-Netz einzudringen, kopiert sich der Wurm in einen Ordner, der zum Dateiaustausch verwendet wird und sich gewöhnlich auf einem PC befindet. Das P2P-Netz zeigt Informationen über diese Datei an. Ein Benutzer kann die infizierte Datei wie andere angebotene Dateien im Netzwerk „finden", herunterladen und öffnen. Komplexere Würmer imitieren das Netzwerkprotokoll eines konkreten P2P-Netzes: Sie antworten positiv auf Suchanfragen und bieten ihre Kopien zum Download an.
Wurm	Sonstige Würmer	Zu den sonstigen Netzwürmern zählen: • Würmer, die ihre Kopien in Netzwerkressourcen verbreiten. Unter Verwendung von Betriebssystemfunktionen durchsuchen sie verfügbare Netzwerkordner, bauen Verbindungen zu Computern im globalen Netzwerk auf und versuchen, umfassenden Zugriff auf ihre Laufwerke zu erhalten. Im Unterschied zu den oben beschriebenen Wurmarten verbreiten sich die sonstigen Würmer nicht selbständig weiter, sondern nur, wenn der Benutzer eine Datei mit einer Wurmkopie öffnet. • Würmer, die nicht zu den in dieser Tabelle beschriebenen Verbreitungsmethoden gehören (z. B. Würmer, die sich über Mobiltelefone weiterverbreiten).

- Trojanische Programme

Subkategorie: trojanische Programme (Trojan_programs)

Bedrohungsstufe: hoch

Im Gegensatz zu Würmern und Viren erstellen trojanische Programme keine Kopien von sich. Sie dringen z. B. über E-Mails oder über den Browser in den Computer ein, wenn der Benutzer eine infizierte Webseite besucht. Trojanische Programme werden unter Beteiligung des Benutzers gestartet. Unmittelbar nach ihrem Start beginnen sie mit ihren schädlichen Aktionen.

Jeder Trojaner-Typ zeigt ein individuelles Verhalten auf dem infizierten Computer. Die Hauptfunktionen von trojanischen Programmen sind das Sperren, Verändern oder Vernichten von Informationen sowie das Hervorrufen von Funktionsstörungen in Computern oder Computernetzwerken. Außerdem können trojanische Programme Dateien empfangen oder senden, Dateien ausführen, auf dem Bildschirm Meldungen anzeigen, auf Webseiten zugreifen, Programme herunterladen und installieren, und einen Computer neu starten.

Häufig verwenden Angreifer eine „Kombination“ aus unterschiedlichen Trojanerprogrammen.

Die folgende Tabelle unterscheidet die Typen der trojanischen Programme nach ihrem Verhalten.

Typen der trojanischen Programme nach ihrem Verhalten auf einem infizierten Computer

Typ	Name	Beschreibung
Trojan-ArcBomb	Trojanische Programme – „Archivbomben”	Archive. Beim Extrahieren vergrößert sich der Inhalt so stark, dass es auf dem Computer zu Funktionsstörungen kommt. Wenn der Benutzer versucht, ein solches Archiv zu entpacken, kann es sein, dass die Leistung des Computers sinkt, der Computer hängen bleibt oder die Festplatte mit „leeren“ Daten überfüllt wird. Eine besondere Gefahr bilden „Archivbomben“ für Datei- und Mailserver. Wird auf dem Server ein System zur automatischen Verarbeitung eingehender Daten verwendet, kann eine „Archivbombe“ den Server zum Absturz bringen.
Backdoor	Trojanische Programme zur Remote-Administration	Dieser Typ gilt unter den trojanischen Programmen als der gefährlichste. Sie gleichen funktionsmäßig Programmen, die zur Remote-Administration auf einem Computer installiert werden. Diese Programme installieren sich auf dem Computer, ohne dass der Benutzer etwas davon bemerkt, und ermöglichen dem Angreifer die Fernsteuerung des Computers.
Trojan	Trojanische Programme	Dieser Typ umfasst folgende schädlichen Programme: • **Klassische trojanische Programme**. Diese Programme führen nur die Grundfunktionen trojanischer Programme aus: Sperrung, Veränderung oder Zerstörung von Informationen, Störung der Arbeit von Computern oder Computernetzwerken. Sie besitzen keine Zusatzfunktionen, über die

		andere Trojaner-Typen verfügen, die in dieser Tabelle beschrieben sind. • **"Mehrzweck"-Trojaner**. Sie besitzen Zusatzfunktionen, die gleichzeitig für mehrere Typen trojanischer Programme charakteristisch sind.
Trojan-Ransom	Trojanische Erpressungsprogramme	Sie nehmen die Daten auf einem PC als „Geisel", indem sie diese verändern oder sperren, oder stören die Arbeit des Computers, damit der Benutzer nicht mehr auf seine Daten zugreifen kann. Der Angreifer fordert vom Benutzer ein Lösegeld und verspricht, dafür ein Programm zu liefern, das die Funktionsfähigkeit des Computers und der Daten wiederherstellt.
Trojan-Clicker	Trojanische Clicker-Programme	Diese Programme greifen von einem PC aus auf Webseiten zu: Sie senden entweder selbst Befehle an den Browser oder ersetzen Webadressen, die in Systemdateien gespeichert sind. Mithilfe dieser Programme organisieren Angreifer Netzwerkangriffe oder steigern die Besucherzahlen von Seiten, um die Anzeigehäufigkeit von Werbebannern zu erhöhen.
Trojan-Downloader	Trojanische Download-Programme	Sie greifen auf die Webseite des Eindringlings zu, laden von dort andere bösartige Programme herunter und installieren sie auf dem Computer des Benutzers. Sie können den Dateinamen des böswilligen Programms enthalten, die heruntergeladen oder von der Webseite, auf die zugegriffen wird, empfangen werden soll.
Trojan-Dropper	Trojanische Installationsprogramme	Nachdem sie auf der Computerfestplatte gespeichert wurden, installieren sie andere trojanische Programme, die sich in ihrem Körper befinden. Angreifer können trojanische Installationsprogramme zu folgenden Zwecken verwenden: • um ohne Wissen des Benutzers ein schädliches Programm zu installieren: Trojanische Installationsprogramme zeigen keinerlei Meldungen an oder blenden falsche Meldungen über einen Fehler im Archiv oder eine inkorrekte Version des Betriebssystems ein. • um andere bekannte Schadsoftware vor der Entdeckung zu schützen: Nicht alle Antiviren-Programme können Schadsoftware in trojanischen Installationsprogrammen erkennen.
Trojan-Notifier	Trojanische Benachrichtigungsprogramme	Sie informieren einen Angreifer darüber, dass der infizierte Computer „online" ist und übermitteln

		folgende Informationen über den Computer: IP-Adresse, Nummer des offenen Ports oder E-Mail-Adresse. Sie nehmen per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise Kontakt mit dem Angreifer auf. Trojanische Benachrichtigungsprogramme werden häufig in Kombination mit unterschiedlichen Trojanerprogrammen eingesetzt. Sie teilen dem Angreifer mit, dass andere trojanische Programme erfolgreich auf einem PC installiert wurden.
Trojan-Proxy	Trojanische Proxy-Programme	Sie ermöglichen es einem Angreifer, über einen PC anonym auf Webseiten zuzugreifen. Sie dienen häufig zum Spam-Versand.
Trojan-PSW	Trojanische Programme zum Kennwortdiebstahl	Trojanische Programme, die Kennwörter stehlen (Password Stealing Ware). Sie berauben Benutzerkonten und stehlen beispielsweise Registrierungsdaten für Softwareprodukte. Sie durchsuchen Systemdateien und die Registrierung nach vertraulichen Daten und schicken diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. Einige dieser trojanischen Programme werden speziellen Typen zugeordnet, die in dieser Tabelle beschrieben sind. Dazu zählen Trojaner, die Bankkonten berauben (Trojan-Banker), Daten von IM-Clients stehlen (Trojan-IM) und Daten aus Netzwerkspielen entwenden (Trojan-GameThief).
Trojan-Spy	Trojanische Spyware-Programme	Sie spionieren den Benutzer aus und sammeln Informationen über die Aktionen, die der Benutzer bei der Arbeit am Computer ausführt. Sie können die Daten abfangen, die der Benutzer über die Tastatur eingibt, Screenshots machen oder Listen aktiver Programme sammeln. Die gesammelten Informationen werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-DDoS	Trojanische Programme für Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung). Häufig werden mehrere Computer von solchen Programmen infiziert, um sie dann gleichzeitig für einen gezielten Angriff auf einen Server zu verwenden. DoS-Programme realisieren einen Angriff von einem Computer aus, wobei der Benutzer davon weiß. DDoS-Programme (Distributed DoS) verwenden eine größere Anzahl von Computern ohne Wissen der Benutzer für verteilte Angriffe.
Trojan-IM	Trojanische Programme zum	Sie stehlen Nummern und Kennwörter der

	Diebstahl der Daten von IM-Client-Benutzern	Benutzer von IM-Clients. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Rootkit	Rootkits	Sie maskieren andere bösartige Programme und deren Aktivität und verlängern so die Persistenz der Programme im Betriebssystem. Sie können auch Dateien, Prozesse im Speicher eines infizierten Computers oder Registrierungsschlüssel, die bösartige Programme ausführen, verbergen. Die Rootkits können den Datenaustausch zwischen Programmen auf dem Computer des Benutzers und anderen Computern im Netzwerk maskieren.
Trojan-SMS	Trojanische Programme für SMS-Nachrichten	Sie infizieren Handys und versenden SMS-Nachrichten an kostenpflichtige Nummern.
Trojan-GameThief	Trojanische Programme zum Diebstahl von Benutzerdaten aus Netzwerkspielen	Sie stehlen Kontodaten von Benutzern, die an Netzwerkspielen für Computer teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Banker	Trojanische Programme zum Diebstahl von Daten über Bankkonten	Sie stehlen Daten über Bankkonten oder über Konten bei elektronischen Zahlungssystemen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Mailfinder	Trojanische Programme, die E-Mail-Adressen sammeln	Sie sammeln auf einem Computer E-Mail-Adressen und übermitteln diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. An die gesammelten Adressen kann der Angreifer Spam verschicken.

- Schädliche Tools

Subkategorie: schädliche Tools (Malicious_tools)

Gefahrenstufe: mittel

Im Gegensatz zu anderen Arten von Malware führen bösartige Tools ihre Aktionen nicht sofort nach dem Start aus. Sie können auf dem Computer des Benutzers sicher gespeichert und gestartet werden. Angreifer verwenden die Funktionen dieser Programme, um Viren, Würmer und Trojaner zu erstellen, Netzwerkangriffe gegen Remote-Server zu organisieren, Computer zu „hacken“ und andere schädliche Aktionen durchzuführen.

Die folgende Tabelle kategorisiert die unterschiedlichen Funktionen von schädlichen Tools.

Funktionen von schädlichen Tools

Typ	Name	Beschreibung
Constructor	Konstrukteure	Mit ihrer Hilfe können neue Viren, Würmer und trojanische Programme erstellt werden. Einige Konstrukteure verfügen über eine standardmäßige Fensteroberfläche, in der über ein Menü der Typ einer zu erstellenden Schadsoftware, die Methode zur Debugger-Abwehr und sonstige Eigenschaften gewählt werden.
Dos	Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung).
Exploit	Exploits	Exploits bestehen aus einer Datenkombination oder aus Programmcode, der die Schwachstellen eines Programms, in dem er verarbeitet wird, ausnutzt, um auf dem Computer eine schädliche Aktion auszuführen. Ein Exploit kann beispielsweise Dateien schreiben oder lesen oder auf „infizierte“ Webseiten zugreifen. Es gibt verschiedene Arten von Exploits, die Schwachstellen unterschiedlicher Programme oder Netzwerkdienste ausnutzen. Exploits werden in Form eines Netzwerkpakets über ein Netzwerk an mehrere Computer übertragen, um Computer mit anfälligen Netzwerkdiensten zu finden. Ein Exploit in einer DOC-Datei nutzt die Schwachstellen eines Textverarbeitungsprogramms. Er kann damit beginnen, die vom Angreifer programmierten Funktionen auszuführen, sobald der Benutzer eine infizierte Datei öffnet. Ein Exploit, der in eine E-Mail-Nachricht eingebettet ist, sucht nach Schwachstellen in einem Mail-Client. Er kann mit der Ausführung einer schädlichen Aktion beginnen, sobald der Benutzer die infizierte E-Mail in diesem Mail-Client öffnet.

		Mithilfe von Exploits werden Netzwürmer (Net-Worm) verbreitet. Nuker-*Exploits*(Nuker) bestehen aus Netzwerkpaketen, die einen Computer zum Absturz bringen.
FileCryptor	Verschlüsselungsprogramme	Chiffreure verschlüsseln schädliche Programme, um sie vor Antiviren-Programmen zu verstecken.
Flooder	Programme zur „Verunreinigung“ von Netzwerken	Sie versenden eine hohe Anzahl von Nachrichten über Netzwerkkanäle. Zu diesem Typ zählen beispielsweise Programme, die der Verunreinigung von Internet Relay Chats dienen. Programme, die der Verunreinigung von Kanälen für E-Mail, IM-Clients und Mobilfunksysteme dienen, zählen nicht zu diesem Typ. Diese Programme werden separaten Typen zugeordnet, die ebenfalls in dieser Tabelle beschrieben sind (Email-Flooder, IM-Flooder und SMS-Flooder).
HackTool	Hacker-Tools	Sie können die Kontrolle über den Computer, auf dem sie installiert sind, übernehmen oder einen anderen Computer angreifen (z. B. ohne Erlaubnis des Benutzers andere Systembenutzer hinzufügen und Systemberichte löschen, um ihre Spuren im System zu verwischen). Zu diesem Typ gehören bestimmte Sniffer, die über schädliche Funktionen wie z. B. das Abfangen von Kennwörtern verfügen. Sniffer (Sniffers) sind Programme, die den Netzwerkverkehr abhören können.
Hoax	Böse Scherze	Diese Programme erschrecken einen Benutzer mit virenähnlichen Meldungen: Sie zeigen fiktive Meldungen über Virenfunde in sauberen Dateien oder über das Formatieren der Festplatte an.
Spoofer	Imitator-Tools	Sie senden E-Mails und Netzwerkanfragen mit gefälschten Absenderadressen. Imitatoren werden beispielsweise von Angreifern verwendet, um einen falschen Absender vorzutäuschen.
VirTool	Tools zur Modifikation schädlicher Programme	Sie erlauben es, andere schädliche Programme so zu modifizieren, dass sie sich vor Antiviren-Programmen verstecken können.
Email-Flooder	Programme zur „Verunreinigung“ von E-Mail-Postfächern	Sie versenden eine hohe Anzahl von Nachrichten an E-Mail-Adressen (“verstopfen diese mit Müll“). Die große Menge von E-Mails hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
IM-Flooder	Programme zur „Verunreinigung“ von IM-Clients	Sie versenden eine hohe Anzahl von Nachrichten an Benutzer von IM-Clients Das hohe Nachrichtenaufkommen hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
SMS-Flooder	Programme zur „Verunreinigung“ von SMS-Systemen	Sie versenden eine große Anzahl von SMS-Nachrichten an Mobiltelefone.

- Adware

Unterkategorie: Adware

Bedrohungsstufe: mittel

Adware-Programme dienen dazu, dem Benutzer Werbung zu zeigen. Sie zeigen auf der Oberfläche anderer Programme Werbebanner an oder leiten Suchanfragen auf Webseiten mit Werbung um. Einige von ihnen sammeln auf Werbung bezogene Informationen über den Benutzer und leiten sie an ihren Urheber weiter, z.B. Informationen darüber, welche Webseiten der Benutzer besucht und welche Suchanfragen er vornimmt. Im Gegensatz zu trojanischer Spyware leiten Adware-Programme diese Informationen mit der Erlaubnis des Benutzers weiter.

- Dialer

Unterkategorie: legale Programme, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gefahrenstufe: mittel

Die Mehrzahl dieser Programme sind nützliche Programme. Sie werden von vielen Anwendern eingesetzt. Dazu zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für die Dienste FTP, HTTP oder Telnet.

Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf einem PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Dialer	Dialer	Dialer können heimlich Telefonverbindungen über ein Modem herstellen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern. Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer

		installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- Andere Programme, mit denen Kriminelle Ihren Computer oder persönliche Daten beschädigen können

Unterkategorie: legale Programme, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gefahrenstufe: mittel

Die Mehrzahl dieser Programme sind nützliche Programme. Sie werden von vielen Anwendern eingesetzt. Dazu zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für die Dienste FTP, HTTP oder Telnet.

Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf einem PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Dialer	Dialer	Dialer können heimlich Telefonverbindungen über ein Modem herstellen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern. Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer

		installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- **Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kann**

  Kaspersky Endpoint Security untersucht gepackte Objekte und das SFX-Modul von selbstentpackenden SFX-Archiven (self-extracting archive).

  Angreifer packen gefährliche Programme mit speziellen Packern oder sie packen Objekte mehrfach, um sie vor Anti-Virus zu verstecken.

  Die Virenanalysten von Kaspersky haben analysiert, welche Packer am häufigsten von Angreifern eingesetzt werden.

  Erkennt Kaspersky Endpoint Security in einem Objekt einen solchen Packer, enthält dieser aller Wahrscheinlichkeit nach ein Schadprogramm oder ein Programm, das von einem Angreifer zur Schädigung des Computers oder der Daten des Benutzers verwendet werden kann.

  Kaspersky Endpoint Security erkennt folgende Programme:

  - *Gepackte Dateien, die Schaden verursachen können* – Solche Dateien dienen zum Packen von Schadprogrammen wie Viren, Würmern und Trojanern.
  - *Mehrfach gepackte Dateien* (mittlerer Bedrohungsgrad) – Dies sind Objekte, die dreimal mit einem oder mehreren Packprogrammen gepackt wurden.

- **Mehrfach gepackte Dateien**

Kaspersky Endpoint Security untersucht gepackte Objekte und das SFX-Modul von selbstentpackenden SFX-Archiven (self-extracting archive).

Angreifer packen gefährliche Programme mit speziellen Packern oder sie packen Objekte mehrfach, um sie vor Anti-Virus zu verstecken.

Die Virenanalysten von Kaspersky haben analysiert, welche Packer am häufigsten von Angreifern eingesetzt werden.

Erkennt Kaspersky Endpoint Security in einem Objekt einen solchen Packer, enthält dieser aller Wahrscheinlichkeit nach ein Schadprogramm oder ein Programm, das von einem Angreifer zur Schädigung des Computers oder der Daten des Benutzers verwendet werden kann.

Kaspersky Endpoint Security erkennt folgende Programme:

- *Gepackte Dateien, die Schaden verursachen können* – Solche Dateien dienen zum Packen von Schadprogrammen wie Viren, Würmern und Trojanern.
- *Mehrfach gepackte Dateien* (mittlerer Bedrohungsgrad) – Dies sind Objekte, die dreimal mit einem oder mehreren Packprogrammen gepackt wurden.

4. Speichern Sie die vorgenommenen Änderungen.

Technologie zur aktiven Desinfektion aktivieren und deaktivieren

Wenn Kaspersky Endpoint Security die Ausführung eines bestimmten Schadsoftware-Abschnitts nicht verhindern kann, können Sie die Technologie zur aktiven Desinfektion verwenden. Die „Aktive Desinfektion“ ist standardmäßig deaktiviert, da diese Technologie die Computerressourcen stark beansprucht. Sie können die „Aktive Desinfektion“ aktivieren, wenn Sie mit aktiven Bedrohungen arbeiten.

Die „Aktive Desinfektion“ funktioniert auf Workstations und Servern in unterschiedlicher Weise. Um die Technologie auf Servern zu verwenden, müssen Sie die sofortige aktive Desinfektion in den Eigenschaften der Aufgabe *Antiviren-Untersuchung* aktivieren. Diese Voraussetzung ist nicht erforderlich, um die Technologie auf Workstations zu verwenden.

Um die Technologie zur aktiven Desinfektion zu aktivieren und zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Aktivieren oder deaktivieren Sie im Abschnitt **Schutzmodus** das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**, um die Technologie zur aktiven Desinfektion zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Während die „Aktive Desinfektion“ ausgeführt wird, kann der Benutzer die meisten Betriebssystemfunktionen nicht verwenden. Wenn die Desinfektion abgeschlossen wird, wird der Computer neu gestartet.

Energiesparmodus aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um den Energiesparmodus zu aktivieren oder zu deaktivieren:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Bedrohungen und Ausnahmen**.
3. Verwenden Sie im Abschnitt **Leistung** das Kontrollkästchen **Geplante Aufgaben bei Batteriebetrieb verschieben**, um den Energiesparmodus zu aktivieren oder zu deaktivieren.

   Ist der Energiesparmodus aktiviert, so werden bei Akkubetrieb folgende Aufgaben auch dann nicht gestartet, wenn ein Startzeitplan dafür vorhanden ist:

   - Update-Aufgabe
   - Aufgabe zur vollständigen Untersuchung
   - Aufgabe zur Untersuchung wichtiger Bereiche
   - Aufgabe zur benutzerdefinierten Untersuchung
   - Aufgabe zur Integritätsprüfung
4. Speichern Sie die vorgenommenen Änderungen.

Freigabe von Ressourcen für andere Programme aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um den Modus zu aktivieren oder zu deaktivieren, in dem Ressourcen für andere Programme freigegeben werden:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Verwenden Sie im Abschnitt **Leistung** das Kontrollkästchen **Ressourcen anderen Programmen zuweisen**, um die Zuweisung von Ressourcen an andere Programme zu aktivieren oder zu deaktivieren.

   Ist der Modus zur Freigabe von Ressourcen für andere Programme aktiviert, schiebt Kaspersky Endpoint Security die Ausführung von Aufgaben auf, wenn sie nach Zeitplan gestartet werden sollen und ihre Ausführung andere Programme verlangsamt:

   - Update-Aufgabe
   - Aufgabe zur vollständigen Untersuchung
   - Aufgabe zur Untersuchung wichtiger Bereiche
   - Aufgabe zur benutzerdefinierten Untersuchung
   - Aufgabe zur Integritätsprüfung

   Der Modus zur Freigabe von Ressourcen für andere Programme ist standardmäßig aktiviert.
4. Speichern Sie die vorgenommenen Änderungen.

Konfigurationsdatei erstellen und verwenden

Mithilfe der Konfigurationsdatei für die Einstellungen von Kaspersky Endpoint Security lassen sich folgende Aufgaben lösen:

- Ausführen einer lokalen Installation von Kaspersky Endpoint Security über die Befehlszeile mit zuvor festgelegten Einstellungen.

  Dazu muss die Konfigurationsdatei im gleichen Ordner gespeichert werden, in dem sich das Programmpaket befindet.

- Ausführen einer Remote-Installation von Kaspersky Endpoint Security über Kaspersky Security Center mit zuvor festgelegten Einstellungen.

- Einstellungen für Kaspersky Endpoint Security von einem Computer auf einem anderen übertragen.

Um eine Konfigurationsdatei zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Einstellungen verwalten** aus.
3. Klicken Sie auf **Export**.
4. Geben Sie in dem sich öffnenden Fenster den Pfad zu dem Ort an, an dem Sie die Konfigurationsdatei speichern möchten, und geben Sie ihren Namen ein.

   Um eine Konfigurationsdatei für die lokale Installation oder für die Remote-Installation von Kaspersky Endpoint Security zu verwenden, muss die Datei install.cfg genannt werden.

5. Klicken Sie auf **Speichern**.

Um die Einstellungen für Kaspersky Endpoint Security aus einer Konfigurationsdatei zu importieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Einstellungen verwalten** aus.
3. Klicken Sie auf **Import**.
4. Geben Sie im folgenden Fenster den Pfad der Konfigurationsdatei an.
5. Klicken Sie auf **Öffnen**.

Alle Werte für die Einstellungen von Kaspersky Endpoint Security werden gemäß der ausgewählten Konfigurationsdatei festgelegt.

Standardeinstellungen für das Programm wiederherstellen

Sie können jederzeit die von Kaspersky empfohlenen Einstellungen für Kaspersky Endpoint Security wiederherstellen. Wenn die Einstellungen wiederhergestellt werden, wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** festgelegt.

So stellen Sie die Standardeinstellungen für das Programm wieder her:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Einstellungen verwalten** aus.
3. Klicken Sie auf **Wiederherstellen**.
4. Klicken Sie auf **Speichern**.

Nachrichtenaustausch zwischen Benutzer und Administrator

Die Komponenten Programmkontrolle, Gerätekontrolle, Web-Kontrolle und Adaptive Kontrolle von Anomalien ermöglichen es den Benutzern des lokalen Unternehmensnetzwerks, auf deren Computern das Programm Kaspersky Endpoint Security installiert ist, Nachrichten an den Administrator zu senden.

In folgenden Fällen kann es notwendig sein, dass der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken muss:

- Die Gerätekontrolle hat den Zugriff auf ein Gerät blockiert.

  Eine Nachrichtenvorlage mit einer Zugriffsanfrage für ein blockiertes Gerät steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Gerätekontrolle bereit.

- Die Programmkontrolle hat den Start eines Programms verboten.

  Eine Nachrichtenvorlage mit einer Starterlaubnisanfrage für ein blockiertes Programm steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Programmkontrolle bereit.

- Die Web-Kontrolle hat den Zugriff auf eine Webressource blockiert.

  Eine Nachrichtenvorlage mit einer Zugriffsanfrage für eine blockierte Webressource steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Web-Kontrolle bereit.

Die Methode für den Nachrichtenversand und die Auswahl der Vorlage hängen davon ab, ob auf dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, eine aktive Richtlinie für Kaspersky Security Center vorhanden ist und eine Verbindung mit dem Administrationsserver für Kaspersky Security Center besteht oder nicht. Folgende Szenarien sind möglich:

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, keiner Richtlinie für Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  In diesem Fall können die Nachrichten, die von Benutzern stammen, im Ereignisspeicher von Kaspersky Security Center eingesehen werden (s. folgende Anleitung). Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Offline-Benutzer für Kaspersky Security Center, so ist die Methode für den Nachrichtenversand davon abhängig, ob eine Verbindung mit Kaspersky Security Center besteht:

  - Besteht eine Verbindung mit Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  - Besteht keine Verbindung mit Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  In beiden Fällen werden die Nachrichtenfelder mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

Um eine vom Benutzer stammende Nachricht im Ereignisspeicher von Kaspersky Security Center anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.

   Im Arbeitsbereich von Kaspersky Security Center werden alle Ereignisse angezeigt, die in Kaspersky Endpoint Security aufgetreten sind. Dazu gehören auch Nachrichten an den Administrator, die von Benutzern des lokalen Unternehmensnetzwerks stammen.

3. Um den Ereignisfilter anzupassen, wählen Sie in der Dropdown-Liste **Ereignisse für Auswahl** das Element **Benutzeranfragen**.

4. Wählen Sie eine Nachricht an den Administrator.

5. Klicken Sie rechts im Arbeitsbereich der Verwaltungskonsole auf **Ereigniseigenschaften öffnen**.

Virtuelle Datentresore

Kaspersky Endpoint Security erlaubt die Verschlüsselung von Dateien und Ordnern, die auf lokalen Laufwerken und Wechseldatenträgern gespeichert sind, sowie die Verschlüsselung kompletter Wechseldatenträger und Festplatten. Die Datenverschlüsselung reduziert das Risiko eines Informationsdiebstahls, falls ein Laptop, ein Wechseldatenträger oder eine Festplatte gestohlen wird oder verloren geht, oder falls Dritte oder andere Programme auf Daten zugreifen. Kaspersky Endpoint Security verwendet den Verschlüsselungsalgorithmus Advanced Encryption Standard (AES).

Wenn die Lizenz abgelaufen ist, verschlüsselt das Programm neue Daten nicht mehr. Bereits verschlüsselte Daten bleiben verschlüsselt und es kann weiterhin damit gearbeitet werden. Um neue Daten zu verschlüsseln, muss das Programm mit einer neuen Lizenz aktiviert werden, welche die Verwendung der Verschlüsselung vorsieht.

In den folgenden Fällen kann nicht garantiert werden, dass zuvor die verschlüsselten Dateien auch weiterhin verschlüsselt bleiben: Wenn die Lizenz abgelaufen ist, der Lizenzvertrag verletzt wurde, die Lizenz gelöscht wurde oder das Programm Kaspersky Endpoint Security oder die Verschlüsselungskomponenten vom Computer des Benutzers entfernt wurden. Dies liegt daran, dass einige Programme, wie z. B. Microsoft Office Word, während der Bearbeitung eine temporäre Kopie der Dateien erstellen. Wenn die Originaldatei gespeichert wird, ersetzt die temporäre Kopie die Originaldatei. Ist die Verschlüsselungsfunktionalität auf dem Computer nicht vorhanden oder nicht verfügbar, so bleibt die Datei unverschlüsselt.

Kaspersky Endpoint Security bietet folgende Datenschutzmaßnahmen:

- **Dateiverschlüsselung auf lokalen Festplatten des Computers**. Sie können folgende Listen anlegen: Listen mit Dateien nach Erweiterung oder Erweiterungsgruppen, und Listen mit Ordnern, die sich auf lokalen Laufwerken des Computers befinden. Außerdem können Sie Verschlüsselungsregeln für Dateien definieren, die von bestimmten Programmen erstellt werden. Nachdem die Richtlinie übernommen wurde, verschlüsselt und entschlüsselt Kaspersky Endpoint Security die folgenden Dateien:
  - Dateien, die einzeln zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die in Ordnern gespeichert sind, welche zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die von bestimmten Programmen erstellt werden
- **Wechseldatenträger verschlüsseln**. Sie können eine Standard-Verschlüsselungsregel festlegen, nach der das Programm für alle Wechseldatenträger die gleiche Aktion ausführt. Außerdem können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.

  Die Standard-Verschlüsselungsregel besitzt eine niedrigere Priorität als die Verschlüsselungsregeln, die für bestimmte Wechseldatenträger erstellt wurden. Verschlüsselungsregeln, die für bestimmte Wechseldatenträger unter Angabe eines Gerätemodells erstellt wurden, besitzen eine niedrigere Priorität als Verschlüsselungsregeln, die für Wechseldatenträger unter Angabe einer Geräte-ID erstellt wurden.

  Um zu wählen, welche Regel für die Dateiverschlüsselung auf einem Wechseldatenträger gilt, überprüft Kaspersky Endpoint Security, ob Gerätemodell und Geräte-ID bekannt sind. Anschließend führt das Programm eine der folgenden Aktionen aus:
  - Ist nur das Gerätemodell bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, falls eine solche Regel vorhanden ist.
  - Ist nur die Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist.
  - Sind Gerätemodell und Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist. Ist eine solche

Regel nicht vorhanden, es gibt aber eine Verschlüsselungsregel, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, so verwendet das Programm diese Regel. Wurde weder für diese Geräte-ID noch für dieses Gerätemodell eine Verschlüsselungsregel festgelegt, so verwendet das Programm die standardmäßige Verschlüsselungsregel.

- Wenn weder das Gerätemodell noch die Geräte-ID bekannt ist, wendet das Programm die Standard-Verschlüsselungsregel an.

Ein Wechseldatenträger kann vom Programm so vorbereitet werden, dass die darauf verschlüsselten Dateien im portablen Modus verwendet werden können. Ist der portable Modus aktiviert, so können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

- **Verwaltung von Regeln für den Zugriff von Programmen auf verschlüsselte Dateien**. Sie können für ein beliebiges Programm eine Regel für den Zugriff auf verschlüsselte Dateien erstellen. Diese Regel kann entweder den Zugriff auf verschlüsselte Dateien verbieten oder nur den Zugriff auf den verschlüsselten Text erlauben, also auf eine Zeichenfolge, die aus der Verschlüsselung hervorgeht.

- **Verschlüsselte Archive erstellen**. Sie können verschlüsselte Archive erstellen und den Zugriff darauf mit einem Kennwort schützen. Der Zugriff auf den Inhalt verschlüsselter Archive wird erst nach Eingabe der Kennwörter gewährt, mit denen Sie den Zugriff auf diese Archive geschützt haben. Solche Archive können gefahrlos über das Internet oder auf Wechseldatenträgern übertragen werden.

- **Vollständige Festplattenverschlüsselung**. Sie können ein Verschlüsselungsverfahren auswählen: Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung (im Folgenden auch „BitLocker“ genannt).

  Die Technologie *BitLocker* ist Bestandteil des Betriebssystems Windows. Wenn ein Computer mit Trusted Platform Module (TPM) ausgerüstet ist, verwendet BitLocker das TPM zur Speicherung von Wiederherstellungsschlüsseln, die zur Freigabe verschlüsselter Festplatten dienen. Beim Hochfahren des Computers fragt BitLocker bei Trusted Platform Module die Wiederherstellungsschlüssel für die Festplatte ab und entsperrt die Festplatte. Sie können die Verwendung eines Kennworts und/oder eines PIN-Codes für den Zugriff auf die Wiederherstellungsschlüssel festlegen.

  Sie können eine standardmäßige Regel für die vollständige Festplattenverschlüsselung festlegen und eine Liste mit Festplatten erstellen, die von der Verschlüsselung ausgeschlossen werden sollen. Nachdem die Richtlinie für Kaspersky Security Center übernommen wurde, führt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung sektorbasiert aus. Das Programm verschlüsselt alle logischen Partitionen der Festplatten auf einmal.

  Nach der Verschlüsselung von Systemfestplatten und einem nachfolgenden Neustart des Computers, sind der Zugriff auf die Festplatten und das Laden des Betriebssystems erst möglich, nachdem der Benutzer sich mithilfe des Authentifizierungsagenten authentifiziert hat. Dazu ist entweder die Eingabe des Kennworts für den Token oder die Smartcard, die mit dem Computer verbunden sind, oder die Eingabe von Benutzername und Kennwort für das Authentifizierungsagenten-Benutzerkonto erforderlich, das vom Systemadministrator des lokalen Unternehmensnetzwerks mithilfe der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* erstellt wurde. Diese Konten basieren auf den Benutzerkonten von Microsoft Windows, mit denen sich die Benutzer im Betriebssystem anmelden. Sie können auch das Verfahren zur Einmalanmeldung (SSO, Single Sign-On) nutzen. Es ermöglicht eine automatische Anmeldung im Betriebssystem mit dem Benutzernamen und dem Kennwort des Authentifizierungsagenten-Benutzerkontos.

  Wenn für den Computer eine Sicherungskopie erstellt wurde, die Computerdaten dann verschlüsselt wurden, anschließend die Sicherungskopie des Computers wiederhergestellt wurde und die Computerdaten erneut verschlüsselt wurden, so erstellt Kaspersky Endpoint Security Duplikate der Benutzerkonten für den Authentifizierungsagenten. Um die Duplikate zu löschen, muss das Dienstprogramm klmover mit dem Parameter `dupfix` verwendet werden. Das Tool gehört zum Lieferumfang von Kaspersky Security Center. Weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Security Center.

Der Zugriff auf verschlüsselte Festplatten ist nur von jenen Computern aus möglich, auf denen das Programm Kaspersky Endpoint Security installiert ist und die vollständige Festplattenverschlüsselung verfügbar ist. Diese Bedingung gewährleistet ein minimales Risiko von Datendiebstahl von der verschlüsselten Festplatte, falls diese außerhalb des lokalen Unternehmensnetzwerks verwendet wird.

Um Festplatten und Wechseldatenträger zu verschlüsseln, können Sie die Funktion **Nur belegten Speicherplatz verschlüsseln** verwenden. Es wird empfohlen, diese Funktion nur für neue Geräte zu verwenden, die bisher noch nicht benutzt worden sind. Wenn Sie die Verschlüsselung auf einem Gerät verwenden möchten, das bereits benutzt wurde, so sollte das gesamte Gerät verschlüsselt werden. Dies garantiert den Schutz aller Daten, selbst gelöschter Daten, aus denen noch Informationen entnommen werden könnten.

Vor dem Beginn der Verschlüsselung erhält Kaspersky Endpoint Security eine Sektorenkarte des Dateisystems. Im ersten Datenstrom werden die Sektoren verschlüsselt, die beim Start der Verschlüsselung mit Dateien belegt sind. Im zweiten Datenstrom werden die Sektoren verschlüsselt, die nach dem Beginn der Verschlüsselung geschrieben wurden. Nach dem Abschluss der Verschlüsselung sind alle Sektoren verschlüsselt, die Daten enthalten.

Löscht der Benutzer nach dem Abschluss der Verschlüsselung eine Datei, so werden die Sektoren, in denen diese Datei gespeichert waren, frei und dort können auf Dateisystemebene Informationen geschrieben werden. Dabei bleiben die Sektoren weiterhin verschlüsselt. Wird die Verschlüsselung regelmäßig ausgeführt und die Funktion **Nur belegten Speicherplatz verschlüsseln** ist aktiviert, so werden durch die kontinuierliche Speicherung von Dateien nach und nach alle Sektoren auf dem neuen Gerät verschlüsselt.

Die Daten, die zur Entschlüsselung von Objekten erforderlich sind, werden vom Administrationsserver für Kaspersky Security Center zur Verfügung gestellt, der den Computer zum Zeitpunkt der Verschlüsselung verwaltet. Kommt ein Computer mit verschlüsselten Objekten unter die Kontrolle eines anderen Administrationsservers, so bestehen folgende Möglichkeiten, um Zugriff auf die verschlüsselten Daten zu erhalten:

- Administrationsserver in derselben Hierarchie:
    - Sie müssen keine zusätzlichen Aktionen ausführen. Der Benutzer kann weiterhin auf die verschlüsselten Objekte zugreifen. Die Chiffrierschlüssel gelten für alle Administrationsserver.
- Die Administrationsserver sind verstreut:
    - Administrator des lokalen Unternehmensnetzwerks um die Freigabe der verschlüsselten Objekte bitten.
    - Daten auf verschlüsselten Geräten mithilfe des Reparatur-Tools wiederherstellen.
    - Aus einer Sicherungskopie die Konfiguration des Administrationsservers für Kaspersky Security Center wiederherstellen, von welchem der Computer bei der Verschlüsselung verwaltet wurde, und diese Konfiguration auf dem Administrationsserver verwenden, welcher den Computer mit den verschlüsselten Objekten verwaltet.

Wenn der Zugriff auf verschlüsselte Daten nicht möglich ist, folgen Sie den entsprechenden Anleitungen für die Arbeit mit verschlüsselten Daten (Wiederherstellen des Zugriffs auf verschlüsselte Dateien, Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht).

Beschränkungen der Verschlüsselungsfunktionalität

Die Datenverschlüsselung besitzt die folgenden Beschränkungen:

- Im Verlauf der Verschlüsselung legt das Programm Verwaltungsdateien an. Für deren Speicherung sind etwa 0,5% unfragmentierter freier Speicherplatz auf der Festplatte des Computers erforderlich. Ist auf der Festplatte zu wenig unfragmentierter Speicherplatz verfügbar, so wird die Verschlüsselung erst gestartet, wenn entsprechende Bedingungen vorliegen.

- Alle Komponenten für Datenverschlüsselung können über die Kaspersky Security Center Verwaltungskonsole und die Kaspersky Security Center 12 Web Console verwaltet werden. Über die Kaspersky Security Center Cloud Console können Sie nur Bitlocker verwalten.

- Die Datenverschlüsselung ist nur verfügbar, wenn Kaspersky Endpoint Security mit dem Administrationssystem Kaspersky Security Center oder Kaspersky Security Center Cloud Console (nur BitLocker) verwendet wird. Eine Datenverschlüsselung ist nicht möglich, wenn Kaspersky Endpoint Security im Offline-Modus verwendet wird, da Kaspersky Endpoint Security die Chiffrierschlüssel in Kaspersky Security Center speichert.

- Ist das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Microsoft Windows für Server installiert, so ist nur die vollständige Festplattenverschlüsselung mithilfe der Technologie BitLocker-Laufwerkverschlüsselung verfügbar. Ist das Programm Kaspersky Endpoint Security auf einem Computer mit Windows für Workstation installiert, so ist die Funktionalität zur Datenverschlüsselung in vollem Umfang verfügbar.

Die Funktionalität zur vollständigen Festplattenverschlüsselung mit dem Verfahren Kaspersky-Festplattenverschlüsselung ist nicht verfügbar für Festplatten, welche die Hard- und Softwarevoraussetzungen nicht erfüllen.

Die Kompatibilität zwischen der Funktionalität für die vollständige Festplattenverschlüsselung von Kaspersky Endpoint Security und Kaspersky Anti-Virus für UEFI wird nicht unterstützt. Kaspersky Anti-Virus für UEFI wird vor dem Hochfahren des Betriebssystems gestartet. Bei der vollständigen Festplattenverschlüsselung erkennt das Programm, dass auf dem Computer kein Betriebssystem installiert ist. Als Folge wird Kaspersky Anti-Virus für UEFI mit einem Fehler beendet. Die Verschlüsselung von Dateien (FLE) beeinflusst die Funktion von Kaspersky Anti-Virus für UEFI nicht.

Kaspersky Endpoint Security unterstützt die folgenden Konfigurationen:

- HDD-, SSD- und USB-Laufwerke.

  Die Technologie von Kaspersky Disk Encryption (FDE) unterstützt die Arbeit mit SSD bei Aufrechterhaltung der Leistung und Lebensdauer von SSD-Laufwerken.

- Über den Bus angeschlossene Laufwerke: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Über SD- oder MMC-Bus angeschlossene nicht auswechselbare Laufwerke.

- Laufwerke mit 512-Byte-Sektoren.

- Laufwerke mit 4096-Byte-Sektoren, die 512 Byte emulieren.

- Laufwerke mit den folgenden Partitionstypen: GPT, MBR und VBR (Wechseldatenträger).

- Eingebettete Software des UEFI 64- und Legacy-BIOS-Standards.

- Eingebettete Software des UEFI-Standards mit Secure Boot-Unterstützung.

  Secure Boot ist eine Technologie zur Überprüfung digitaler Signaturen für UEFI-Lader-Programme und -Treiber. Secure Boot blockiert den Start von UEFI-Programmen und -Treibern, die unsigniert oder von unbekannten Herausgebern signiert sind. Kaspersky Disk Encryption (FDE) unterstützt Secure Boot vollständig. Der Authentifizierungsagent ist durch ein Microsoft Windows UEFI-Treiber-Publisher-Zertifikat signiert.

  Auf einigen Geräten (z. B. Microsoft Surface Pro und Microsoft Surface Pro 2) kann eine veraltete Liste von Zertifikaten zur Verifizierung digitaler Signaturen standardmäßig installiert sein. Bevor Sie das Laufwerk verschlüsseln können, müssen Sie die Liste der Zertifikate aktualisieren.

- Eingebettete Software des UEFI-Standards mit Fast Boot-Unterstützung.

Fast Boot ist eine Technologie, die dem Computer hilft, schneller zu starten. Wenn die Fast Boot-Technologie aktiviert ist, lädt der Computer normalerweise nur den Mindestsatz an UEFI-Treibern, der zum Starten des Betriebssystems erforderlich ist. Wenn die Fast Boot-Technologie aktiviert ist, funktionieren USB-Tastaturen, Mäuse, USB-Token, Touchpads und Touchscreens möglicherweise nicht, während der Authentifizierungsagent ausgeführt wird.

Um Kaspersky Disk Encryption (FDE) zu verwenden, wird empfohlen, die Fast Boot-Technologie zu deaktivieren. Sie können das FDE-Testprogramm verwenden, um die Funktion von Kaspersky Disk Encryption (FDE) zu testen.

Folgende Konfigurationen werden von Endpoint Security nicht unterstützt:

- Schema, bei dem sich Ladeprogramm und Betriebssystem auf unterschiedlichen Laufwerken befinden
- integrierte Software des Standards UEFI 32
- Das System verfügt über Intel® Rapid Start Technology und Laufwerke, die über eine Hibernation-Partition verfügen, selbst wenn Intel® Rapid Start Technology deaktiviert ist.
- Laufwerke im MBR-Format mit mehr als 10 erweiterten Partitionen.
- Das System verfügt über eine Auslagerungsdatei, die sich auf einem Nicht-Systemlaufwerk befindet.
- Multi-Boot-System mit mehreren gleichzeitig installierten Betriebssystemen.
- dynamische Partitionen (nur primäre Partitionen werden unterstützt)
- Laufwerke, auf denen weniger als 0,5% freier unfragmentierter Speicherplatz vorhanden ist
- Laufwerke mit einer anderen Sektorgröße als 512 Byte oder 4096 Byte mit 512-Byte-Emulation
- Hybridlaufwerke
- Das System verfügt über Fremdlader.
- Laufwerke mit komprimierten NTFS-Verzeichnissen.
- Die Kaspersky Disk Encryption-Technologie (FDE) ist nicht kompatibel mit anderen Festplattenverschlüsselungstechnologien (wie BitLocker, McAfee Drive Encryption und WinMagic SecureDoc).
- Die Kaspersky Disk Encryption-Technologie (FDE) ist mit der Express-Cache-Technologie nicht kompatibel.
- Das Erstellen, Löschen und Ändern von Partitionen auf einem verschlüsselten Laufwerk wird nicht unterstützt. Sie könnten Daten verlieren.
- Dateisystemformatierung wird nicht unterstützt. Sie könnten Daten verlieren.

  Wenn Sie ein Laufwerk formatieren müssen, das mit der FDE-Technologie (Kaspersky Disk Encryption) verschlüsselt wurde, formatieren Sie das Laufwerk auf einem Computer, der nicht über Kaspersky Endpoint Security für Windows verfügt, und verwenden Sie nur die vollständige Festplattenverschlüsselung.

  Ein verschlüsseltes Laufwerk, das mit der Schnellformatierungsoption formatiert wurde, kann fälschlicherweise als verschlüsselt erkannt werden, wenn es das nächste Mal an einen Computer angeschlossen wird, auf dem Kaspersky Endpoint Security für Windows installiert ist. Benutzerdaten werden nicht verfügbar sein.
- Der Authentifizierungsagent unterstützt nicht mehr als 100 Konten.

- Die Single-Sign-On-Technologie ist mit anderen Technologien von anderen Entwicklern nicht kompatibel.
- Die Kaspersky Disk Encryption-Technologie (FDE) wird von den folgenden Gerätemodellen nicht unterstützt:
  - Dell Latitude E6410 (UEFI-Modus)
  - HP Compaq nc8430 (Legacy-BIOS-Modus)
  - Lenovo Think Center 8811 (Legacy-BIOS-Modus)
- Der Authentifizierungsagent unterstützt nicht die Arbeit mit USB-Tokens, wenn die Legacy-USB-Unterstützung aktiviert ist. Auf dem Computer wird nur eine kennwortbasierte Authentifizierung möglich sein.
- Beim Verschlüsseln eines Laufwerks im Legacy-BIOS-Modus wird empfohlen, die Legacy-USB-Unterstützung bei den folgenden Gerätemodellen zu aktivieren:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550

- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (Hauptplatine)

Änderung der Länge des Chiffrierschlüssels (AES56 / AES256)

Kaspersky Endpoint Security verwendet den Verschlüsselungsalgorithmus AES (Advanced Encryption Standard). Kaspersky Endpoint Security unterstützt den AES-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 256 und 56 Bit. Der Algorithmus für die Datenverschlüsselung ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Strong encryption (AES256)* oder *Lite encryption (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

Die Länge des Chiffrierschlüssels kann nur in Kaspersky Endpoint Security 11.2.0 und höher geändert werden.

Die Länge des Chiffrierschlüssels wird in zwei Schritten geändert:

1. Entschlüsseln Sie die Objekte, die mit dem Programm Kaspersky Endpoint Security verschlüsselt wurden, bevor die Länge des Chiffrierschlüssels geändert wird:
   a. Entschlüsseln Sie die Festplatten.
   b. Entschlüsseln Sie die Dateien auf lokalen Datenträgern.
   c. Entschlüsseln Sie die Wechseldatenträger.

   Nachdem die Länge des Chiffrierschlüssels geändert wurde, sind zuvor verschlüsselte Objekte nicht mehr verfügbar.
2. Entfernen Sie Kaspersky Endpoint Security.
3. Installieren Sie Kaspersky Endpoint Security aus dem Programmpaket für Kaspersky Endpoint Security mit der anderen Verschlüsselungsbibliothek.

Sie können die Länge des Chiffrierschlüssels auch durch ein Programm-Update ändern. Um die Länge des Chiffrierschlüssels durch ein Programm-Update zu ändern, müssen die folgenden Bedingungen erfüllt sein:

- Auf dem Computer ist das Programm Kaspersky Endpoint Security Version 10 Service Pack 2 oder höher installiert.

- Die folgenden Komponenten zur Datenverschlüsselung sind nicht auf dem Computer installiert: Dateiverschlüsselung, Vollständige Festplattenverschlüsselung.

  Komponenten zur Datenverschlüsselung gehören standardmäßig nicht zum Umfang von Kaspersky Endpoint Security. Die Komponente „Verwaltung von BitLocker“ hat keinen Einfluss auf eine Änderung der Länge des Chiffrierschlüssels.

Um die Länge des Chiffrierschlüssels zu ändern, starten Sie die Datei kes_win.msi oder setup_kes.exe aus dem Programmpaket mit der entsprechenden Verschlüsselungsbibliothek. Sie können das Programm auch ferngesteuert mithilfe eines Installationspakets aktualisieren.

Es ist nicht möglich, die Länge des Chiffrierschlüssels mithilfe des Programmpakets für die gleiche Programmversion zu ändern, die auf Ihrem Computer installiert ist, ohne das Programm vorher zu entfernen.

Kaspersky-Festplattenverschlüsselung

Die Technologie „Kaspersky-Festplattenverschlüsselung“ ist nur für Computer verfügbar, die ein Windows-Betriebssystem für Workstations verwenden. Verwenden Sie für Computer mit einem Windows-Betriebssystem für Server die Technologie „BitLocker-Laufwerkverschlüsselung“.

Kaspersky Endpoint Security unterstützt die vollständige Festplattenverschlüsselung in den Dateisystemen FAT32, NTFS und exFat.

Bevor die vollständige Festplattenverschlüsselung gestartet wird, überprüft das Programm, ob die Verschlüsselung auf dem Gerät möglich ist. Dabei wird u. a. überprüft, ob die Systemfestplatte mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist. Für die Kompatibilitätsprüfung ist ein Neustart des Computers erforderlich. Nach dem Neustart des Computers nimmt das Programm automatisch alle notwendigen Prüfungen vor. Wenn die Kompatibilitätsprüfung erfolgreich verläuft, startet die vollständige Festplattenverschlüsselung, nachdem das System hochgefahren und das Programm gestartet wurde. Wenn die Überprüfung ergibt, dass die Systemfestplatte nicht mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist, muss der Computer mit dem Reset-Knopf am Computergehäuse neu gestartet werden. Kaspersky Endpoint Security protokolliert Informationen über die Inkompatibilität. Basierend auf diesen Informationen startet das Programm beim Start des Betriebssystems keine vollständige Festplattenverschlüsselung. Die Berichte von Kaspersky Security Center enthalten Informationen über dieses Ereignis.

Wenn die Hardware-Konfiguration des Computers verändert wurde und anschließend die Systemfestplatte auf Kompatibilität mit dem Authentifizierungsagenten und mit der BitLocker-Verschlüsselungskomponente überprüft werden soll, müssen zuerst die Inkompatibilitätsinformationen gelöscht werden, die das Programm bei der vorherigen Überprüfung ermittelt hat. Geben Sie dazu vor der vollständigen Festplattenverschlüsselung in der Befehlszeile folgenden Befehl ein: `avp pbatestreset`. Wenn sich das Betriebssystem nicht mehr hochfahren lässt, nachdem die Kompatibilität der Systemfestplatte mit dem Authentifizierungsagenten überprüft wurde, müssen mithilfe des Reparatur-Tools die Objekte und Daten gelöscht werden, die nach dem Testlauf des Authentifizierungsagenten verblieben sind. Starten Sie danach Kaspersky Endpoint Security und führen Sie erneut den Befehl `avp pbatestreset` aus.

Nach dem Start der vollständigen Festplattenverschlüsselung verschlüsselt Kaspersky Endpoint Security alle Daten, die auf Festplatten geschrieben werden.

Wenn der Benutzer den Computer während der vollständigen Festplattenverschlüsselung ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung nach dem Beenden des Energiesparmodus fort, ohne den Authentifizierungsagenten zu laden.

Es gibt zwei Methoden, mit denen sich der Benutzer im Authentifizierungsagenten authentifizieren kann:

- Durch Eingabe von Name und Kennwort eines Benutzerkontos für den Authentifizierungsagenten, wenn das Benutzerkonto vom Administrator des lokalen Unternehmensnetzwerks mit Mitteln von Kaspersky Security Center erstellt wurde.
- Durch Eingabe des Kennworts für einen Token oder eine Smartcard, die mit dem Computer verbunden sind.

  Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Der Authentifizierungsagent unterstützt Tastaturlayouts für die folgenden Sprachen:

- Englisch (Großbritannien)
- Englisch (USA)
- Arabisch (Algerien, Marokko, Tunesien, AZERTY-Layout)
- Spanisch (Lateinamerika)
- Italienisch
- Deutsch (Deutschland und Österreich)
- Deutsch (Schweiz)
- Portugiesisch (Brasilien, ABNT2-Layout)
- Russisch (für IBM-/Windows-Tastatur mit 105 Tasten und JCUKEN-Tastaturlayout)
- Türkisch (QWERTY-Layout)
- Französisch (Frankreich)
- Französisch (Schweiz)
- Französisch (Belgien, AZERTY-Tastaturlayout)

- Japanisch (für Tastatur mit 106 Tasten und QWERTY-Tastaturlayout)

Ein Tastaturlayout steht im Authentifizierungsagenten zur Verfügung, wenn es in den Einstellungen des Betriebssystems unter Region und Sprache hinzugefügt wurde und auf dem Windows-Begrüßungsbildschirm verfügbar ist.

Wenn der Name des Authentifizierungsagenten-Benutzerkontos Zeichen enthält, die nicht mithilfe der im Authentifizierungsagenten verfügbaren Tastaturlayouts eingegeben werden können, so ist der Zugriff auf verschlüsselte Festplatten erst möglich, nachdem die Festplatten mithilfe des Reparatur-Tools wiederhergestellt wurden oder nachdem der Name und das Kennwort des Authentifizierungsagenten-Benutzerkontos wiederhergestellt wurden.

Besondere Merkmale der SSD-Laufwerksverschlüsselung

Das Programm unterstützt die Verschlüsselung von SSD-Laufwerken, hybriden SSHD-Laufwerken und Laufwerken mit der Intel Smart Response-Funktion. Das Programm unterstützt nicht die Verschlüsselung von Laufwerken mit der Intel Rapid Start Funktion. Deaktivieren Sie die Intel Rapid Start-Funktion vor der Verschlüsselung eines solchen Laufwerks.

Für die Verschlüsselung von SSD-Laufwerken gelten die folgenden Besonderheiten:

- Wenn ein SSD-Laufwerk neu ist und keine vertraulichen Daten enthält, aktivieren Sie die Verschlüsselung nur des belegten Speicherplatzes. Damit können Sie die entsprechenden Laufwerksektoren überschreiben.
- Wenn ein SSD-Laufwerk verwendet wird und vertrauliche Daten enthält, wählen Sie eine der folgenden Optionen:
  - Löschen Sie das SSD-Laufwerk vollständig (Secure Erase), installieren Sie das Betriebssystem und führen Sie die Verschlüsselung des SSD-Laufwerks mit aktivierter Option zur Verschlüsselung nur des belegten Speicherplatzes aus.
  - Führen Sie die Verschlüsselung des SSD-Laufwerks aus, wobei die Option zur Verschlüsselung nur des belegten Speicherplatzes deaktiviert ist.

Die Verschlüsselung eines SSD-Laufwerks erfordert 5-10 GB freien Speicherplatz. Die Anforderungen an den freien Speicherplatz für die Speicherung von Verschlüsselungsverwaltungsdaten sind in der folgenden Tabelle aufgeführt.

Freier Speicherplatzbedarf für die Speicherung von Verschlüsselungsverwaltungsdaten

Größe des SSD-Laufwerks (GB)	Freier Speicherplatz auf der primären Partition des SSD-Laufwerks (MB)	Freier Speicherplatz auf der sekundären Partition des SSD-Laufwerks (MB)
128	250	64
256	250	640
512	300	128

Vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung sicherzustellen, dass der Computer nicht infiziert ist. Starten Sie dazu eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Um eine vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung auszuführen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Element **Kaspersky-Festplattenverschlüsselung** aus.

   Das Verfahren „Kaspersky-Festplattenverschlüsselung“ kann nicht verwendet werden, wenn auf dem Computer Festplatten vorhanden sind, die mithilfe von BitLocker verschlüsselt sind.

7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** den das Element **Alle Festplatten verschlüsseln** aus.

   Wenn auf einem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung aller Festplatten nur noch jenes Betriebssystem ausführen, in dem das Programm installiert ist.

   Wenn bestimmte Festplatten von der Verschlüsselung ausgenommen werden sollen, müssen Sie diese in einer Liste angeben.

8. Konfigurieren Sie Regeln zum Hinzufügen von Benutzerkonten des Authentifizierungsagenten während der Festplattenverschlüsselung. Mithilfe des Agenten können Benutzer die Authentifizierung für den Zugriff auf verschlüsselte Laufwerke durchlaufen und das Betriebssystem laden. Passen Sie die folgenden Einstellungen an, um Benutzerkonten des Authentifizierungsagenten automatisch hinzuzufügen:

   - **Während der Verschlüsselung automatisch Benutzerkonten des Authentifizierungsagenten für Windows-Benutzer erstellen**. Wenn dieses Kontrollkästchen aktiviert ist, erstellt das Programm Benutzerkonten des Authentifizierungsagenten basierend auf der Liste der Windows-Benutzerkonten auf dem Computer. Kaspersky Endpoint Security verwendet standardmäßig alle lokalen und Domänen-Benutzerkonten, mit denen sich der Benutzer in den letzten 30 Tagen am Betriebssystem angemeldet hat.
   - **Bei der Anmeldung automatisch Authentifizierungsagenten-Konten für alle Benutzer dieses Computers erstellen**. Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm Informationen zu Windows-Benutzerkonten auf dem Computer, bevor der Authentifizierungsagent gestartet wird. Wenn Kaspersky Endpoint Security ein Windows-Benutzerkonto erkennt, das kein Benutzerkonto des Authentifizierungsagenten besitzt, erstellt das Programm ein neues Konto für den Zugriff auf verschlüsselte

Laufwerke. Das neue Benutzerkonto des Authentifizierungsagenten verfügt über die folgenden Standardeinstellungen: nur kennwortgeschützte Anmeldung, Kennwortänderung bei der ersten Authentifizierung. Es ist also nicht nötig, für Computer mit bereits verschlüsselten Laufwerken Benutzerkonten des Authentifizierungsagenten manuell mithilfe der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzuzufügen.

Wenn Sie die automatische Erstellung von Benutzerkonten des Authentifizierungsagenten deaktiviert haben, können Sie mithilfe der Aufgabe *Konten verwalten* Benutzerkonten des Authentifizierungsagenten manuell hinzufügen. Mit dieser Aufgabe können Sie außerdem die Einstellungen der automatisch erstellten Benutzerkonten des Authentifizierungsagenten ändern.

9. Der Einfachheit halber kann der Benutzername im Speicher des Authentifizierungsagenten hinterlegt werden, sodass Benutzer bei der nächsten Anmeldung im System nur noch das Kennwort eingeben müssen. Aktivieren Sie dazu das Kontrollkästchen **Benutzernamen speichern, der im Authentifizierungsagenten eingegeben wurde**.

10. Wählen Sie eine der folgenden Verschlüsselungsmethoden:

    - Damit nur die Festplattensektoren verschlüsselt werden, die mit Dateien belegt sind, aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.

      Verwenden Sie die Verschlüsselung auf einem Datenträger, der bereits benutzt wurde, so sollte der gesamte Datenträger verschlüsselt werden. Dies garantiert den Schutz aller Daten, selbst gelöschter Daten, aus denen noch Informationen entnommen werden könnten. Die Funktion **Nur belegten Speicherplatz verschlüsseln** wird für neue Datenträger empfohlen, die bisher noch nicht benutzt wurden.

    - Damit die gesamte Festplatte verschlüsselt wird, deaktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.

      Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, so werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Alle Festplatten verschlüsseln** übernommen wurde.

11. Wenn bei der Verschlüsselung des Computers ein Kompatibilitätsproblem mit der Hardware auftritt, können Sie das Kontrollkästchen **Legacy USB Support verwenden** aktivieren.

    Legacy USB Support **ist eine** BIOS-/UEFI-Funktion, die es ermöglicht, USB-Geräte (z. B. ein Token) zu verwenden, wenn der Computer gestartet wird und das Betriebssystem noch nicht gestartet wurde (BIOS-Modus). Nach dem Start des Betriebssystems beeinflusst die Funktion „Legacy USB Support“ die Unterstützung von USB-Geräten nicht mehr.

    Wenn die Funktion „Legacy USB Support“ aktiviert ist, unterstützt der Authentifizierungsagent im BIOS-Modus die Verwendung von USB-Tokens nicht. Die Funktion sollte nur beim Auftreten von Hardware-Kompatibilitätsproblemen verwendet werden und ausschließlich für jene Computer aktiviert werden, auf welchen das Problem aufgetreten ist.

12. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool "Encryption Monitor" kann über das Programmhauptfenster ausgeführt werden.

Sind die Systemfestplatten verschlüsselt, so wird vor dem Laden des Betriebssystems der Authentifizierungsagent geladen. Authentifizieren Sie sich mithilfe des Authentifizierungsagenten, damit die verschlüsselten Systemfestplatten freigegeben werden und das Betriebssystem hochgefahren wird. Nach erfolgreicher Authentifizierung wird das Betriebssystem hochgefahren. Bei jedem nachfolgenden Neustart des Betriebssystems ist eine erneute Authentifizierung erforderlich.

Liste mit Festplatten erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen

Eine Ausnahmeliste für die Verschlüsselung kann nur für das Verfahren „Kaspersky-Festplattenverschlüsselung“ erstellt werden.

Gehen Sie wie folgt vor, um eine Liste mit Festplatten zu erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Variante **Kaspersky-Festplattenverschlüsselung**.

   In der Tabelle **Folgende Festplatten nicht verschlüsseln** werden Einträge mit Festplatten angezeigt, die nicht vom Programm verschlüsselt werden. Wenn Sie noch keine Liste mit Festplatten für die Ausnahme aus der Verschlüsselung erstellt haben, ist diese Tabelle leer.
7. Gehen Sie wie folgt vor, um der Liste mit Festplatten neue Festplatten hinzuzufügen, die nicht vom Programm verschlüsselt werden sollen:

   a. Klicken Sie auf **Hinzufügen**.

      Das Fenster **Geräte aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

   b. Geben Sie im Fenster **Geräte aus der Liste für Kaspersky Security Center hinzufügen** Werte für die Einstellungen **Name**, **Computer**, **Datenträgertyp**, **Kaspersky-Festplattenverschlüsselung** an.

   c. Klicken Sie auf **Aktualisieren**.

   d. Aktivieren Sie in der Spalte **Name** die Kontrollkästchen in den Tabellenzeilen für jene Festplatten, die zur Liste der nicht zu verschlüsselnden Festplatten hinzugefügt werden sollen.

   e. Klicken Sie auf **OK**.

   Die ausgewählten Festplatten werden in der Tabelle **Folgende Festplatten nicht verschlüsseln** angezeigt.
8. Um Festplatten aus der Ausnahmetabelle zu löschen, wählen Sie in der Tabelle **Folgende Festplatten nicht verschlüsseln** eine oder mehrere Zeilen und klicken Sie auf **Löschen**.

Um in der Tabelle mehrere Zeilen zu wählen, halten Sie die Taste **STRG** gedrückt.

9. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste von Festplatten, die von der Verschlüsselung ausgenommen wurden

Sie können die Liste der Ausnahmen der Festplattenverschlüsselung in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um die Listen der überwachten Ports zu sichern oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen der Festplattenverschlüsselung in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Variante **Kaspersky-Festplattenverschlüsselung**.

   In der Tabelle **Folgende Festplatten nicht verschlüsseln** werden Einträge mit Festplatten angezeigt, die nicht vom Programm verschlüsselt werden.
7. So exportieren Sie die Liste der Ausnahmen:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
8. So importieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
9. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste von Ausnahmen der Festplattenverschlüsselung in der Web Console

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste von Erweiterungen exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie **Virtuelle Datentresore → Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **Kaspersky-Festplattenverschlüsselung** aus und klicken Sie auf den Link, um zu den Einstellungen zu wechseln.

   Die Verschlüsselungseinstellungen werden geöffnet.
6. Klicken Sie auf **Ausnahmen**.
7. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.
   d. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   e. Klicken Sie auf **Speichern**.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
8. So importieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
9. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Technologie zur Einmalanmeldung (SSO) aktivieren

Das Verfahren zur Einmalanmeldung (SSO, Single Sign-On) ermöglicht eine automatische Anmeldung am Betriebssystem mithilfe der Anmeldedaten des Authentifizierungsagenten.

Wenn das Verfahren zur Einmalanmeldung verwendet wird, ignoriert der Authentifizierungsagent die Anforderungen an die Kennwortkomplexität, die in Kaspersky Security Center festgelegt sind. Die Anforderungen an die Kennwortkomplexität können Sie in den Betriebssystemeinstellungen festlegen.

Das Verfahren zur Einmalanmeldung ist inkompatibel mit Drittanbietern von Anmeldedaten.

Verwendung des Verfahrens zur Einmalanmeldung in der Verwaltungskonsole (MMC) aktivieren

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Allgemeine Verschlüsselungseinstellungen** aus.
6. Klicken Sie im Block **Einstellungen für Kennwörter** auf die Schaltfläche **Einstellungen**.
7. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Authentifizierungsagent** das Kontrollkästchen **Technologie zur Einmalanmeldung (SSO) verwenden**.
8. Speichern Sie die vorgenommenen Änderungen.

Dadurch muss der Benutzer die Authentifizierung mithilfe des Agenten nur ein Mal durchlaufen. Für den Start des Betriebssystems ist kein Authentifizierungsvorgang erforderlich. Das Betriebssystem wird automatisch gestartet.

In der „Web Console“ die Verwendung des Verfahrens zur Einmalanmeldung aktivieren

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Verwendung des Verfahrens zur Einmalanmeldung aktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **Kaspersky-Festplattenverschlüsselung** aus und klicken Sie auf den Link, um zu den Einstellungen zu wechseln.

   Die Verschlüsselungseinstellungen werden geöffnet.
6. Aktivieren Sie im Block **Einstellungen für Kennwörter** das Kontrollkästchen **Technologie zur Einmalanmeldung (SSO) verwenden**.
7. Klicken Sie auf **OK**.

Dadurch muss der Benutzer die Authentifizierung mithilfe des Agenten nur ein Mal durchlaufen. Für den Start des Betriebssystems ist kein Authentifizierungsvorgang erforderlich. Das Betriebssystem wird automatisch gestartet.

Damit das Verfahren zur Einmalanmeldung funktioniert, müssen das Kennwort des Windows-Kontos und das Kennwort des Authentifizierungsagenten-Benutzerkontos identisch sein. Wenn die Kennwörter unterschiedlich sind, muss der Benutzer die Authentifizierung zwei Mal ausführen: auf der Benutzeroberfläche des Authentifizierungsagenten und vor dem Start des Betriebssystems. Anschließend ersetzt Kaspersky Endpoint Security das Kennwort des Authentifizierungsagenten-Benutzerkontos mit dem Kennwort des Windows-Kontos.

Authentifizierungsagenten-Konten verwalten

Der Authentifizierungsagent wird benötigt, um mit Datenträgern zu arbeiten, die mithilfe der Technologie Kaspersky-Festplattenverschlüsselung (FDE) verschlüsselt sind. Der Benutzer muss vor dem Start des Betriebssystems die Authentifizierung mithilfe des Agenten durchlaufen. Die Einstellungen für die Authentifizierung von Benutzern können mit der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* angepasst werden. Sie können sowohl lokale Aufgaben für einzelne Computer als auch Gruppenaufgaben für Computer aus bestimmten Administrationsgruppen oder für bestimmte Computer verwenden.

Für die Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* kann kein Startzeitplan eingerichtet werden. Außerdem kann die Ausführung dieser Aufgabe nicht zwangsweise abgebrochen werden.

Erstellen der Aufgabe „Benutzerkonten des Authentifizierungsagenten verwalten“ in der Verwaltungskonsole (MMC)

1. Wechseln Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Aufgaben**.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (11.6.0)** → **Benutzerkonten des Authentifizierungsagenten verwalten** aus.

Schritt 2. Befehl für die Verwaltung der Authentifizierungsagenten-Benutzerkonten auswählen

Erstellen Sie eine Liste mit den Befehlen für die Verwaltung der Authentifizierungsagenten-Benutzerkonten. Mit Verwaltungsbefehlen kann ein Authentifizierungsagenten-Benutzerkonto hinzugefügt, geändert oder gelöscht werden (s. Anleitung unten). Nur jene Benutzer, die ein Authentifizierungsagenten-Benutzerkonto haben, können den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Schritt 3. Auswahl der Geräte, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgabe ein, z. B. `Benutzerkonten für Administratoren`.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Erstellen der Aufgabe „Benutzerkonten des Authentifizierungsagenten verwalten“ in der „Web Console“

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Programm** den Punkt **Kaspersky Endpoint Security für Windows (11.6.0)** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Authentifizierungsagenten-Konten verwalten** aus.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise `Benutzerkonten für Administratoren`.
4. Wählen Sie im Block **Geräte auswählen, denen die Aufgabe zugewiesen wird** den Gültigkeitsbereich der Aufgabe aus.

Schritt 2. Benutzerkonten des Authentifizierungsagenten verwalten

Erstellen Sie eine Liste mit den Befehlen für die Verwaltung der Authentifizierungsagenten-Benutzerkonten. Mit Verwaltungsbefehlen kann ein Authentifizierungsagenten-Benutzerkonto hinzugefügt, geändert oder gelöscht werden (s. Anleitung unten). Nur jene Benutzer, die ein Authentifizierungsagenten-Benutzerkonto haben, können den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Schritt 3. Aufgabenerstellung abschließen

Beenden Sie den Assistenten durch Klick auf **Fertig**. Die neue Aufgabe wird in der Aufgabenliste angezeigt.

Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Start**, um die Aufgabe auszuführen.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Um ein Authentifizierungsagenten-Benutzerkonto hinzuzufügen, muss ein spezieller Befehl zur Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um auf allen Computern ein Administratorkonto hinzuzufügen.

In Kaspersky Endpoint Security können vor der Datenträgerverschlüsselung automatisch Authentifizierungsagenten-Benutzerkonten erstellt werden. Sie können das automatische Erstellen von Authentifizierungsagenten-Benutzerkonten in den Einstellungen der Richtlinie für die vollständige Festplattenverschlüsselung aktivieren. Sie können auch das Verfahren zur Einmalanmeldung (SSO) verwenden.

Hinzufügen eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten*.

2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen** aus.

3. Klicken Sie auf **Hinzufügen** → **Befehl zum Hinzufügen eines Benutzerkontos**.

4. Geben Sie im folgenden Fenster im Feld **Windows-Benutzerkonto** den Namen des Microsoft Windows-Kontos an, auf dessen Basis das Authentifizierungsagenten-Benutzerkonto erstellt werden soll.

5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* mit einem Fehler abgeschlossen.

6. Aktivieren Sie das Kontrollkästchen **Vorhandenes Benutzerkonto ersetzen**, wenn Sie möchten, dass ein bereits für den Authentifizierungsagenten erstelltes Benutzerkonto mit demselben Namen durch das neu hinzugefügte Benutzerkonto ersetzt wird.

   > Dieser Schritt ist verfügbar, wenn Sie den Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten in den Eigenschaften einer Gruppenaufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten hinzufügen. Dieser Schritt ist nicht verfügbar, wenn Sie den Befehl zur Erstellung eines Authentifizierungsagenten-Kontos in den Eigenschaften der lokalen Aufgabe **Gesamten Datenträger verschlüsseln, Benutzerkonten verwalten** hinzufügen.

7. Geben Sie im Feld **Benutzername** den Namen des Benutzerkontos für den Authentifizierungsagenten ein, der zur Authentifizierung für den Zugriff auf verschlüsselte Festplatten dient.

8. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen.

9. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten dazu auffordert, einen Token oder eine Smartcard mit dem Computer zu verbinden. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus.

10. Geben Sie erforderlichenfalls im Feld **Beschreibung des Befehls** die Informationen des Benutzerkontos für den Authentifizierungsagenten ein, welche Sie für die Verwendung des Befehls benötigen.

11. Führen Sie eine der folgenden Aktionen aus:

    - Wählen Sie die Variante **Authentifizierung zulassen** aus, damit das Programm einem Benutzer, welcher bei dem im Befehl angegebenen Benutzerkonto angemeldet ist, den Zugriff auf die Anmeldung im Authentifizierungsagenten erlaubt.

- Wählen Sie die Variante **Authentifizierung verbieten** aus, damit das Programm einem Benutzer, welcher bei dem im Befehl angegebenen Benutzerkonto angemeldet ist, den Zugriff auf die Anmeldung im Authentifizierungsagenten verbietet.

12. Speichern Sie die vorgenommenen Änderungen.

[Hinzufügen eines Authentifizierungsagenten-Benutzerkontos über „Web Console"]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Klicken Sie in der Liste der Authentifizierungsagenten-Benutzerkonten auf **Hinzufügen**.

   Der Assistent zur Verwaltung von Authentifizierungsagenten-Benutzerkonten wird gestartet.

5. Wählen Sie den Befehlstyp **Benutzerkonto hinzufügen** aus.

6. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen. Klicken Sie auf **Weiter**.

   Kaspersky Endpoint Security ermittelt die Sicherheits-ID des Benutzerkontos (SID, Security Identifier). Dies ist für die Überprüfung des Benutzerkontos erforderlich. Wenn Sie den Benutzernamen falsch eingegeben haben, schließt Kaspersky Endpoint Security die Aufgabe mit einem Fehler ab.

7. Passen Sie die Einstellungen des Authentifizierungsagenten-Benutzerkontos an.

   - **Neues Authentifizierungsagenten-Benutzerkonto erstellen anstelle des vorhandenen Kontos**. Kaspersky Endpoint Security überprüft die vorhandenen Authentifizierungsagent-Benutzerkonten auf dem Computer. Wenn die Sicherheits-ID des Benutzers auf dem Computer und in der Aufgabe übereinstimmen, ändert Kaspersky Endpoint Security die Benutzerkonto-Einstellungen in Übereinstimmung mit der Aufgabe.

   - **Benutzername**. Der Benutzername des Authentifizierungsagenten-Benutzerkontos entspricht standardmäßig dem Domänennamen des Benutzers.

   - **Anmeldung mit Kennwort erlauben**. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen. Dadurch hat jeder Benutzer ein einmaliges Kennwort. Außerdem können Sie in der Richtlinie die Anforderungen an die Kennwortkomplexität für das Authentifizierungsagenten-Benutzerkonto festlegen.

   - **Anmeldung mit Zertifikat erlauben**. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus. Dadurch wird festgelegt, dass der Benutzer das Kennwort der Smartcard oder des Tokens eingeben muss.

   - **Zugriff des Benutzerkontos auf verschlüsselte Daten**. Passen Sie den Zugriff des Benutzers auf einen verschlüsselten Datenträger an. Sie können beispielsweise die Benutzerauthentifizierung vorübergehend verbieten, ohne das Authentifizierungsagenten-Benutzerkonto zu löschen.

   - **Kommentar**. Geben Sie bei Bedarf eine Beschreibung für das Benutzerkonto ein.

8. Speichern Sie die vorgenommenen Änderungen.

9. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Um das Kennwort und andere Einstellungen des Authentifizierungsagenten-Benutzerkontos zu ändern, muss ein spezieller Befehl zur Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um das Token-Zertifikat des Administrators auf allen Computern zu ändern.

Ändern eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten*.
2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen** aus.
3. Klicken Sie auf **Hinzufügen → Befehl zum Ändern eines Benutzerkontos**.
4. Geben Sie im folgenden Fenster **Windows-Benutzerkonto** den Namen des Microsoft Windows-Benutzerkontos an, das Sie ändern möchten.
5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* mit einem Fehler abgeschlossen.

6. Aktivieren Sie das Kontrollkästchen **Benutzername ändern** und geben Sie einen neuen Namen für das Benutzerkonto des Authentifizierungsagenten ein, damit Kaspersky Endpoint Security den Benutzernamen in den Namen aus dem darunter angebrachten Feld ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.
7. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Kennwort ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem Kennwort zu erhalten.
8. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest.
9. Aktivieren Sie das Kontrollkästchen **Regel für die Kennwortänderung bei der Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security den Wert für die Kennwortänderung in den darunter angegebenen Wert ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.
10. Legen Sie einen Wert für die Kennwortänderung bei der Anmeldung über den Authentifizierungsagenten fest.
11. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Zertifikat ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem elektronischen Token- oder Smartcard-Zertifikat zu erhalten.
12. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort für einen angeschlossenen Token oder eine Smartcard abfragt. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus.
13. Aktivieren Sie das Kontrollkästchen **Beschreibung des Befehls ändern** und ändern Sie die Beschreibung des Befehls, damit Kaspersky Endpoint Security die Beschreibung ändert. Die Änderung erfolgt für alle

Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

14. Aktivieren Sie das Kontrollkästchen **Regel für den Zugriff auf die Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security die Zugriffsregel für die Anmeldung über den Authentifizierungsagenten in die darunter angegebene Regel ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

15. Legen Sie eine Regel für den Zugriff auf die Authentifizierung im Authentifizierungsagenten fest.

16. Speichern Sie die vorgenommenen Änderungen.

[Ändern eines Authentifizierungsagenten-Benutzerkontos über „Web Console"]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Klicken Sie in der Liste der Authentifizierungsagenten-Benutzerkonten auf **Hinzufügen**.

   Der Assistent zur Verwaltung von Authentifizierungsagenten-Benutzerkonten wird gestartet.

5. Wählen Sie den Befehlstyp **Benutzerkonto ändern** aus.

6. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen. Klicken Sie auf **Weiter**.

   Kaspersky Endpoint Security ermittelt die Sicherheits-ID des Benutzerkontos (SID, Security Identifier). Dies ist für die Überprüfung des Benutzerkontos erforderlich. Wenn Sie den Benutzernamen falsch eingegeben haben, schließt Kaspersky Endpoint Security die Aufgabe mit einem Fehler ab.

7. Aktivieren Sie die Kontrollkästchen neben den Einstellungen, die Sie ändern möchten.

8. Passen Sie die Einstellungen des Authentifizierungsagenten-Benutzerkontos an.

   - **Neues Authentifizierungsagenten-Benutzerkonto erstellen anstelle des vorhandenen Kontos**. Kaspersky Endpoint Security überprüft die vorhandenen Authentifizierungsagent-Benutzerkonten auf dem Computer. Wenn die Sicherheits-ID des Benutzers auf dem Computer und in der Aufgabe übereinstimmen, ändert Kaspersky Endpoint Security die Benutzerkonto-Einstellungen in Übereinstimmung mit der Aufgabe.

   - **Benutzername**. Der Benutzername des Authentifizierungsagenten-Benutzerkontos entspricht standardmäßig dem Domänennamen des Benutzers.

   - **Anmeldung mit Kennwort erlauben**. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen. Dadurch hat jeder Benutzer ein einmaliges Kennwort. Außerdem können Sie in der Richtlinie die Anforderungen an die Kennwortkomplexität für das Authentifizierungsagenten-Benutzerkonto festlegen.

   - **Anmeldung mit Zertifikat erlauben**. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus. Dadurch wird festgelegt, dass der Benutzer das Kennwort der Smartcard oder des Tokens eingeben muss.

   - **Zugriff des Benutzerkontos auf verschlüsselte Daten**. Passen Sie den Zugriff des Benutzers auf einen verschlüsselten Datenträger an. Sie können beispielsweise die Benutzerauthentifizierung vorübergehend verbieten, ohne das Authentifizierungsagenten-Benutzerkonto zu löschen.

   - **Kommentar**. Geben Sie bei Bedarf eine Beschreibung für das Benutzerkonto ein.

9. Speichern Sie die vorgenommenen Änderungen.

10. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

Um ein Authentifizierungsagenten-Benutzerkonto zu löschen, muss ein spezieller Befehl zur Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um das Benutzerkonto eines entlassenen Mitarbeiters zu löschen.

Löschen eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten*.
2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen** aus.
3. Klicken Sie auf **Hinzufügen** → **Befehl zum Löschen eines Benutzerkontos**.
4. Geben Sie im folgenden Fenster im Feld **Windows-Benutzerkonto** den Namen des Windows-Kontos an, auf dessen Basis das zu löschende Authentifizierungsagenten-Benutzerkonto erstellt wurde.
5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* mit einem Fehler abgeschlossen.

6. Speichern Sie die vorgenommenen Änderungen.

Löschen eines Authentifizierungsagenten-Benutzerkontos über „Web Console"

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.

4. Klicken Sie in der Liste der Authentifizierungsagenten-Benutzerkonten auf **Hinzufügen**.

   Der Assistent zur Verwaltung von Authentifizierungsagenten-Benutzerkonten wird gestartet.

5. Wählen Sie den Befehlstyp **Benutzerkonto löschen** aus.

6. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen.

7. Speichern Sie die vorgenommenen Änderungen.

8. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

   Nachdem die Aufgabe ausgeführt wurde, kann der Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang nicht durchlaufen und das Betriebssystem nicht starten. Kaspersky Endpoint Security verbietet den Zugriff auf die verschlüsselten Daten.

Eine Liste der Benutzer, welche die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten können, können Sie in den Eigenschaften des verwalteten Computers einsehen.

Anzeigen einer Liste der Authentifizierungsagenten-Benutzerkonten über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.

5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Aufgaben** aus.

   Die Liste der lokalen Aufgaben wird geöffnet.

6. Wählen Sie die Aufgaben **Benutzerkonten des Authentifizierungsagenten verwalten** aus.

7. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen** aus.

   Eine Liste der Authentifizierungsagenten-Benutzerkonten auf diesem Computer wird angezeigt. Nur die Benutzer aus dieser Liste können die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten.

Anzeigen einer Liste der Authentifizierungsagenten-Benutzerkonten über „Web Console“

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Verwaltete Geräte** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die Liste der Authentifizierungsagenten-Benutzerkonten einsehen möchten.

   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Aufgaben** aus.

   Die Liste der lokalen Aufgaben wird geöffnet.
4. Wählen Sie die Aufgaben **Benutzerkonten des Authentifizierungsagenten verwalten** aus.
5. Wählen Sie in den Aufgabeneigenschaften die Registerkarte **Programmeinstellungen** aus.

Eine Liste der Authentifizierungsagenten-Benutzerkonten auf diesem Computer wird angezeigt. Nur die Benutzer aus dieser Liste können die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten.

Verwendung eines Tokens oder einer Smartcard bei der Arbeit mit dem Authentifizierungsagenten

Bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten kann ein Token oder eine Smartcard verwendet werden. Dazu muss die Datei des elektronischen Token- oder Smartcard-Zertifikats zur Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzugefügt werden.

Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Kaspersky Endpoint Security unterstützt folgende Tokens, Smartcard-Lesegeräte und Smartcards:

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K (Java)
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511

- Rutoken ECP
- Rutoken ECP Flash
- Aladdin-RD JaCarta PKI
- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI

Um die Datei des elektronischen Zertifikats für einen Token oder eine Smartcard zu dem Befehl hinzuzufügen, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, muss die Datei zuerst mithilfe des Zertifikatsverwaltungsprogramms eines Drittanbieters gespeichert werden.

Das Zertifikat für den Token oder die Smartcard muss folgende Eigenschaften besitzen:

- Das Zertifikat entspricht dem Standard X.509 und die Zertifikatsdatei besitzt die Codierung DER.
- Das Zertifikat enthält einen RSA-Schlüssel mit einer Mindestlänge von 1024 Bit.

Wenn das elektronische Token- oder Smartcard-Zertifikat diese Voraussetzungen nicht erfüllt, ist es nicht möglich, die Zertifikatsdatei in den Befehl zu laden, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird.

Außerdem muss der Parameter `KeyUsage` des Zertifikats den Wert `keyEncipherment` oder `dataEncipherment` besitzen. Der Parameter `KeyUsage` bestimmt den Zweck des Zertifikats. Wenn der Parameter einen anderen Wert hat, lädt Kaspersky Security Center die Zertifikatsdatei zwar, es erscheint aber eine Warnung.

Hat der Benutzer den Token oder die Smartcard verloren, so muss der Administrator die elektronische Zertifikatdatei des neuen Tokens oder der neuen Smartcard zum Befehl für das Erstellen des Authentifizierungsagenten-Benutzerkontos hinzufügen. Anschließend muss der Benutzer den Vorgang zur Freigabe von verschlüsselten Geräten oder zur Datenwiederherstellung auf verschlüsselten Geräten durchführen.

Entschlüsselung von Festplatten

Sie können Festplatten auch dann entschlüsseln, wenn keine aktuelle Lizenz vorliegt, welche die Datenverschlüsselung zulässt.

Gehen Sie folgendermaßen vor, um Festplatten zu entschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung** aus.

6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Verfahren, mit dem die Festplatten verschlüsselt wurden.

7. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Alle Festplatten entschlüsseln**, wenn Sie alle verschlüsselten Festplatten entschlüsseln möchten.

   - Fügen Sie in der Tabelle **Folgende Festplatten nicht verschlüsseln** alle verschlüsselten Festplatten hinzu, die Sie entschlüsseln möchten.

     Diese Variante ist nur für das Verschlüsselungsverfahren „Kaspersky-Festplattenverschlüsselung“ verfügbar.

8. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool "Encryption Monitor" kann über das Programmhauptfenster ausgeführt werden.

Wenn der Benutzer während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, den Computer ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort.

Wechselt das Betriebssystem während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort. Nach der Entschlüsselung der Festplatten ist der Ruhezustand erst wieder verfügbar, nachdem das Betriebssystem neu gestartet wurde.

Wechselt das Betriebssystem während der Festplattenentschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security beim Beenden des Energiesparmodus die Festplattenentschlüsselung fort, ohne den Authentifizierungsagenten zu laden.

Wiederherstellen des Zugriffs auf einen Datenträger, der mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist

Wenn der Benutzer das Kennwort für den Zugriff auf eine Festplatte vergessen hat, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, muss ein Wiederherstellungsvorgang (“Anfrage-Frage“) ausgeführt werden.

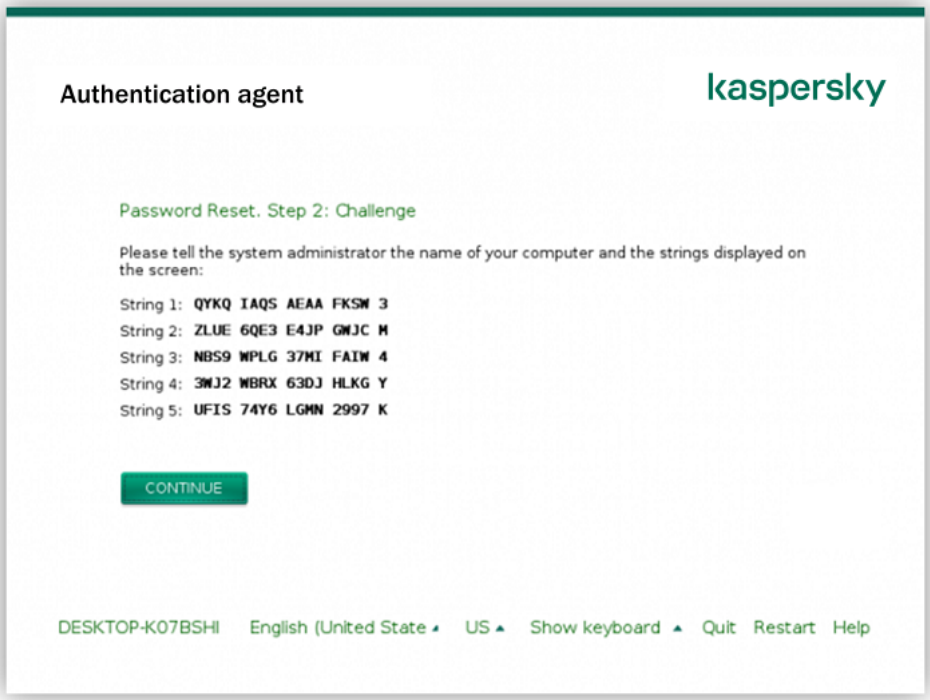
Wiederherstellen des Zugriffs auf eine Systemfestplatte

Um den Zugriff auf eine Systemfestplatte wiederherzustellen, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, sind folgende Schritte erforderlich:

1. Der Benutzer übermittelt die Anfrageblöcke an den Administrator (s. Abb. unten).

2. Der Administrator gibt die Anfrageblöcke in Kaspersky Security Center ein, erhält Antwortblöcke und übermittelt die Antwortblöcke an den Benutzer.

3. Der Benutzer gibt die Antwortblöcke auf der Benutzeroberfläche des Authentifizierungsagenten ein und erhält Zugriff auf die Festplatte.



Wiederherstellen des Zugriffs auf eine Systemfestplatte, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf der Benutzeroberfläche des Authentifizierungsagenten auf die Schaltfläche **Kennwort vergessen** klicken.

[In der Verwaltungskonsole (MMC) die Antwortblöcke für eine Systemfestplatte anfordern, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist]

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der die Wiederherstellung des Zugriffs auf verschlüsselte Daten anfordert, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Authentifizierungsagent** aus.
7. Wählen Sie im Block **Verwendeter Verschlüsselungsalgorithmus** einen Verschlüsselungsalgorithmus aus: **AES56** oder **AES256**.

   Der Algorithmus für die Datenverschlüsselung ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Strong encryption (AES256)* oder *Lite encryption (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.
8. Wählen Sie in der Dropdown-Liste **Benutzerkonto** das Authentifizierungsagenten-Konto des Benutzers aus, der die Zugriffswiederherstellung für das Laufwerk angefordert hat.
9. Wählen Sie in der Dropdown-Liste **Festplatte** die verschlüsselte Festplatte, auf welche der Zugriff wiederhergestellt werden soll.
10. Geben Sie im Abschnitt **Benutzeranfrage** die Anfrageblöcke ein, die der Benutzer diktiert hat.

    Im Feld **Zugriffsschlüssel** wird der Inhalt der Antwortblöcke für die Benutzeranfrage angezeigt, die der Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto dient. Übermitteln Sie den Inhalt der Antwortblöcke an den Benutzer.

[In der „Web Console“ die Antwortblöcke für eine Systemfestplatte anfordern, die mit der Technologie „Kaspersky-Festplattenverschlüsselung“ geschützt ist]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Verwaltete Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.
4. Wählen Sie im folgenden Fenster den Abschnitt **Authentifizierungsagent** aus.
5. Wählen Sie in der Liste **Benutzerkonto** den Namen des Authentifizierungsagenten-Benutzerkontos, das für jenen Benutzer erstellt wurde, der die Wiederherstellung des Benutzernamens und Kennworts für das Authentifizierungsagenten-Benutzerkonto beantragt hat.
6. Geben Sie die Anfrageblöcke ein, die Ihnen der Benutzer diktiert hat.

   Der Inhalt der Antwortblöcke für die Benutzeranfrage, die zur Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto dient, wird im unteren Fensterbereich angezeigt. Übermitteln Sie den Inhalt der Antwortblöcke an den Benutzer.

Nach erfolgreichem Wiederherstellungsvorgang fordert der Authentifizierungsagent den Benutzer auf, das Kennwort zu ändern.

Wiederherstellen des Zugriffs auf eine Nicht-Systemfestplatte

Um den Zugriff auf eine Nicht-Systemfestplatte wiederherzustellen, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, sind die folgenden Schritte erforderlich:

1. Der Benutzer sendet eine Zugriffsanfrage-Datei an den Administrator.
2. Der Administrator fügt die Zugriffsanfrage-Datei in Kaspersky Security Center hinzu, erstellt eine Zugriffsschlüsseldatei und sendet diese Datei an den Benutzer.
3. Der Benutzer fügt die Zugriffsschlüsseldatei in Kaspersky Endpoint Security hinzu und erhält Zugriff auf die Festplatte.

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf die Festplatte zugreifen. Dann erstellt Kaspersky Endpoint Security eine Zugriffsanfrage-Datei (Datei mit der Erweiterung kesdc), die beispielsweise per E-Mail an den Administrator übermittelt werden muss.

In der Verwaltungskonsole (MMC) eine Zugriffsschlüsseldatei für eine verschlüsselte Nicht-Systemfestplatte anfordern

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der die Wiederherstellung des Zugriffs auf verschlüsselte Daten anfordert, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Datenverschlüsselung** aus.
7. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.
8. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.

In der „Web Console“ eine Zugriffsschlüsseldatei für eine verschlüsselte Nicht-Systemfestplatte anfordern

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Verwaltete Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.
4. Wählen Sie den Abschnitt **Datenverschlüsselung** aus.
5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.
6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Update des Betriebssystems

Ein Update des Betriebssystems eines Computers, der mithilfe der vollständigen Festplattenverschlüsselung (FDE) geschützt ist, besitzt bestimmte Besonderheiten. Gehen Sie beim Update des Betriebssystems schrittweise vor: Aktualisieren Sie zuerst das Betriebssystem auf einem Computer, dann auf einigen weiteren Computern, und schließlich auf allen Computern des Netzwerks.

Wenn Sie die Kaspersky-Verschlüsselungstechnologie verwenden, wird vor dem Systemstart der „Authentifizierungsagent" geladen. Mithilfe des „Authentifizierungsagenten" meldet sich der Benutzer beim System an und erhält Zugriff auf die verschlüsselten Datenträger. Danach beginnt der Start des Betriebssystems.

Wenn das Update des Betriebssystems auf einem Computer gestartet wird, der mithilfe der Technologie „Kaspersky-Festplattenverschlüsselung" geschützt ist, so kann der Betriebssystem-Update-Assistent den „Authentifizierungsagenten" entfernen. Dadurch kann der Computer blockiert werden, da das Betriebssystem-Ladeprogramm nicht auf den verschlüsselten Datenträger zugreifen kann.

Details über das sichere Update des Betriebssystems finden Sie in der Wissensdatenbank des Technischen Supports.

Das automatische Update des Betriebssystems ist unter den folgenden Bedingungen verfügbar:

1. Betriebssystem-Update über WSUS (Windows Server Update Services).
2. Auf dem Computer ist das Betriebssystem Windows 10 Version 1607 (RS1) oder höher installiert.
3. Auf dem Computer ist das Programm Kaspersky Endpoint Security Version 11.2.0 oder höher installiert.

Wenn alle Bedingungen erfüllt sind, können Sie das Betriebssystem wie gewöhnlich aktualisieren.

Wenn Sie die Technologie von Kaspersky Disk Encryption (FDE) verwenden und Kaspersky Endpoint Security für Windows Version 11.1.0 oder 11.1.1 auf dem Computer installiert ist, brauchen Sie die Festplatten nicht zu entschlüsseln, um Windows 10 zu aktualisieren.

Um das Betriebssystem zu aktualisieren, müssen Sie Folgendes tun:

1. Bevor Sie das System aktualisieren, kopieren Sie die Treiber mit den Namen cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf und klfdefsf.sys in einen lokalen Ordner. Zum Beispiel C:\fde_drivers.
2. Führen Sie die System-Update-Installation mit dem Parameter `/ReflectDrivers` aus und geben Sie den Ordner mit den gespeicherten Treibern an:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

Wenn Sie die BitLocker-Verschlüsselungstechnologie verwenden, müssen die Festplatten nicht entschlüsselt werden, um Windows 10 zu aktualisieren. Details über BitLocker finden Sie auf der *Microsoft-Website*.

Behebung von Fehlern beim Upgrade der Verschlüsselungsfunktionalität

Beim Programm-Upgrade von einer Vorgängerversion auf die Version Kaspersky Endpoint Security für Windows 11.6.0 wird die Funktionalität zur vollständigen Festplattenverschlüsselung aktualisiert.

Beim Start des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung können folgende Fehler auftreten:

- Das Update konnte nicht initialisiert werden.
- Das Gerät ist mit dem Authentifizierungsagenten nicht kompatibel.

Um Fehler zu beheben, die beim Start des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung aufgetreten sind, gehen Sie in der neuen Programmversion wie folgt vor:

1. Entschlüsseln Sie die Festplatten.
2. Verschlüsseln Sie die Festplatten erneut.

Beim Upgrade der Funktionalität für die vollständige Festplattenverschlüsselung können folgende Fehler auftreten:

- Das Update konnte nicht abgeschlossen werden.
- Das Upgrade der Verschlüsselungsfunktionalität wurde mit einem Fehler abgeschlossen.

Um Fehler zu beheben, die im Verlauf des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung aufgetreten sind,

stellen Sie den Zugriff auf das verschlüsselte Gerät mithilfe des Reparatur-Tools wieder her.

Protokollierungsstufe für den Authentifizierungsagenten wählen

Das Programm zeichnet folgende Informationen in einer Protokolldatei auf: Dienstinformationen über die Verwendung des Authentifizierungsagenten und Informationen über die Benutzeraktionen im Authentifizierungsagenten.

Um die Protokollierungsstufe für den Authentifizierungsagenten festzulegen, gehen Sie wie folgt vor:

1. Drücken Sie sofort nach dem Start des Computers, dessen Festplatten verschlüsselt sind, die Taste **F3**, um das Fenster mit den Einstellungen des Authentifizierungsagenten zu öffnen.
2. Wählen Sie im Konfigurationsfenster des Authentifizierungsagenten eine Protokollierungsstufe aus:
   - **Disable debug logging (default)**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei keine Informationen über die Ereignisse des Authentifizierungsagenten.
   - **Enable debug logging**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.
   - **Enable verbose logging**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.

     Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Enable debug logging**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.

   - **Enable debug logging and select serial port**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

     Ist der Computer, dessen Festplatten verschlüsselt sind, über den COM-Port mit einem anderen Computer verbunden, so können die Ereignisse des Authentifizierungsagenten mithilfe des anderen Computers verfolgt werden.

- **Enable verbose debug logging and select serial port**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

  Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Enable debug logging and select serial port**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.

Eine Protokolldatei des Authentifizierungsagenten wird dann aufgezeichnet, wenn auf dem Computer verschlüsselte Festplatten vorhanden sind oder wenn die vollständige Festplattenverschlüsselung ausgeführt wird.

Die Protokolldatei des Authentifizierungsagenten wird im Gegensatz zu anderen Protokolldateien für das Programm nicht an Kaspersky übertragen. Falls erforderlich, können Sie die Protokolldatei des Authentifizierungsagenten selbst zur Analyse an Kaspersky schicken.

Hilfetexte für den Authentifizierungsagenten ändern

Bevor Sie die Hilfetexte für den Authentifizierungsagenten ändern, beachten Sie die Liste der Zeichen, die in der Preboot-Umgebung unterstützt werden (s. unten).

Um die Hilfetexte für den Authentifizierungsagenten zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Allgemeine Verschlüsselungseinstellungen** aus.
6. Klicken Sie im Block **Vorlagen** auf **Hilfe**.

   Das Fenster **Hilfetexte für den Authentifizierungsagenten** wird geöffnet.
7. Gehen Sie wie folgt vor:

   - Öffnen Sie die Registerkarte **Authentifizierung**, um den Hilfetext zu ändern, welcher im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem die Anmeldedaten eingegeben werden.
   - Öffnen Sie die Registerkarte **Kennwort ändern**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten geändert wird.
   - Öffnen Sie die Registerkarte **Kennwort wiederherstellen**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten wiederhergestellt wird.
8. Ändern Sie die Hilfetexte.

Um den ursprünglichen Text wiederherzustellen, klicken Sie auf **Standard**.

Der Hilfetext kann maximal 16 Zeilen umfassen. Die maximale Zeilenlänge beträgt 64 Zeichen.

9. Speichern Sie die vorgenommenen Änderungen.

Beschränkungen für die Zeichenunterstützung in Hilfetexten für den Authentifizierungsagenten

In der Preboot-Umgebung werden folgende Unicode-Zeichen unterstützt:

- Basis-Lateinisch (0000 - 007F)
- Lateinisch-1, Ergänzung (0080 - 00FF)
- Lateinisch, erweitert-A (0100 - 017F)
- Lateinisch, erweitert-B (0180 - 024F)
- Spacing Modifier Letters (02B0 - 02FF)
- Kombinierende diakritische Zeichen (0300 - 036F)
- Griechisch und Koptisch (0370 - 03FF)
- Kyrillisch (0400 - 04FF)
- Hebräisch (0590 - 05FF)
- Arabisch (0600 - 06FF)
- Lateinisch, weiterer Zusatz (1E00 - 1EFF)
- Allgemeine Interpunktion (2000 - 206F)
- Währungszeichen (20A0 - 20CF)
- Buchstabenähnliche Symbole (2100 - 214F)
- Geometrische Formen (25A0 - 25FF)
- Arabische Präsentationsformen-B (FE70 - FEFF)

Zeichen, die nicht in dieser Liste angegeben sind, werden in der Preboot-Umgebung nicht unterstützt. Es wird davon abgeraten, solche Zeichen in den Hilfetexten des Authentifizierungsagenten zu verwenden.

Objekte und Daten löschen, die nach dem Testlauf des Authentifizierungsagenten verblieben sind

Wenn bei der Deinstallation des Programms Kaspersky Endpoint Security Objekte und Daten gefunden werden, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind, so wird die Programmdeinstallation abgebrochen und kann erst wieder gestartet werden, nachdem diese Objekte und Daten gelöscht wurden.

Objekte und Daten verbleiben nach einem Testlauf des Authentifizierungsagenten nur in Ausnahmefällen auf der Systemfestplatte. Dies kann beispielsweise vorkommen, wenn der Computer nach dem Übernehmen der Richtlinie für Kaspersky Security Center, die entsprechende Verschlüsselungseinstellungen enthält, noch nicht neu gestartet wurde oder wenn das Programm nach einem Testlauf des Authentifizierungsagenten nicht gestartet wird.

Es gibt folgende Methoden, um Objekte und Daten zu löschen, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind:

- mithilfe der Richtlinie für Kaspersky Security Center
- mithilfe des Reparatur-Tools.

Um die Objekte und Daten, die nach einem Testlauf des Authentifizierungsagenten verblieben sind, mithilfe der Richtlinie für Kaspersky Security Center zu löschen, gehen Sie wie folgt vor:

1. Übernehmen Sie für den Computer die Richtlinie für Kaspersky Security Center mit den Einstellungen, die für die Entschlüsselung aller Computerfestplatten gelten.
2. Starten Sie Kaspersky Endpoint Security.

Um Daten über die Inkompatibilität des Authentifizierungsagenten zu löschen,

geben Sie in der Befehlszeile ein: `avp pbatestreset`.

Verwaltung von BitLocker

BitLocker ist eine integrierte Verschlüsselungstechnologie des Windows-Betriebssystems. Kaspersky Endpoint Security ermöglicht es, BitLocker mithilfe von Kaspersky Security Center zu kontrollieren und zu verwalten. BitLocker verschlüsselt ein logisches Volume. Wechseldatenträger können mithilfe von BitLocker nicht verschlüsselt werden. Details über BitLocker finden Sie in der Microsoft-Dokumentation.

Die Sicherheit beim Speichern von Zugriffsschlüsseln gewährleistet BitLocker mithilfe von Trusted Platform Module. *Trusted Platform Module (TPM)* ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Ein Trusted Platform Module wird normalerweise auf der Hauptplatine des Computers installiert und interagiert mit allen anderen Systemkomponenten über die Hardwareschnittstelle. Die Verwendung des TPM ist die sicherste Art, BitLocker-Zugriffsschlüssel zu speichern, da das TPM eine Überprüfung der Systemintegrität vor dem Systemstart ermöglicht. Auf Computern ohne TPM können Sie Laufwerke verschlüsseln. Dabei wird der Zugriffsschlüssel mit einem Kennwort verschlüsselt. BitLocker verwendet die folgenden Authentifizierungsmethoden:

- TPM.
- TPM und PIN-Code.
- Kennwort.

Nach der Laufwerkverschlüsselung erstellt BitLocker einen Master-Schlüssel. Kaspersky Endpoint Security sendet den Master-Schlüssel an Kaspersky Security Center, damit Sie den Zugriff auf das Laufwerk wiederherstellen können, beispielsweise wenn der Benutzer das Kennwort vergisst.

Wenn der Benutzer mithilfe von BitLocker selbständig ein Laufwerk verschlüsselt hat, sendet Kaspersky Endpoint Security Informationen über die Laufwerksverschlüsselung an Kaspersky Security Center. Den Master-Schlüssel sendet Kaspersky Endpoint Security dabei nicht an Kaspersky Security Center. Darum lässt sich der Zugriff auf das Laufwerk mithilfe von Kaspersky Security Center nicht wiederherstellen. Damit BitLocker mit Kaspersky Security Center ordnungsgemäß funktioniert, entschlüsseln Sie das Laufwerk und verschlüsseln Sie es erneut mithilfe der Richtlinie. Sie können das Laufwerk entweder lokal oder mithilfe der Richtlinie entschlüsseln.

Nachdem die Systemfestplatte verschlüsselt wurde, von der das Betriebssystem gestartet wird, muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach dem Authentifizierungsverfahren ermöglicht BitLocker die Anmeldung von Benutzern. BitLocker unterstützt keine Single-Sign-On-Technologie (SSO).

Wenn Sie Gruppenrichtlinien für Windows verwenden, deaktivieren Sie die BitLocker-Verwaltung in den Richtlinieneinstellungen. Es kann sein, dass die Windows-Richtlinieneinstellungen den Richtlinieneinstellungen von Kaspersky Endpoint Security widersprechen. Bei einer Laufwerksverschlüsselung könnten deshalb Fehler auftreten.

Start der „BitLocker-Laufwerkverschlüsselung"

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung sicherzustellen, dass der Computer nicht infiziert ist. Starten Sie dazu eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Damit BitLocker auf Computern mit einem Windows-Betriebssystem für Server ordnungsgemäß funktioniert, kann die Installation der Komponente „BitLocker-Laufwerkverschlüsselung" erforderlich sein. Installieren Sie die Komponente mithilfe der Betriebssystem-Tools (Assistent zum Hinzufügen von Rollen und Komponenten). Details über die Installation der Komponente „BitLocker-Laufwerkverschlüsselung" finden Sie in der Microsoft-Dokumentation.

So führen Sie die BitLocker-Laufwerkverschlüsselung über die Verwaltungskonsole (MMC) aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Element **BitLocker-Laufwerkverschlüsselung** aus.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** den das Element **Alle Festplatten verschlüsseln** aus.

   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.

8. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung“ an (s. folgende Tabelle).
9. Speichern Sie die vorgenommenen Änderungen.

[So führen Sie die BitLocker-Laufwerkverschlüsselung über die Web Console und die Cloud Console aus]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die „BitLocker-Laufwerkverschlüsselung“ starten möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung**.
5. Wählen Sie im Block **Verschlüsselungsverwaltung** das Element **BitLocker-Laufwerkverschlüsselung** aus.
6. Klicken Sie auf den Link **BitLocker-Laufwerkverschlüsselung**.

   Ein Fenster mit den Einstellungen für die „BitLocker-Laufwerkverschlüsselung“ wird geöffnet.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** den das Element **Alle Festplatten verschlüsseln** aus.

   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.
8. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung“ an (s. folgende Tabelle).
9. Klicken Sie auf **OK**.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool "Encryption Monitor" kann über das Programmhauptfenster ausgeführt werden.

Nach der Anwendung der Richtlinie zeigt das Programm je nach Authentifizierungseinstellungen die folgenden Abfragen an:

- Nur TPM. Keine Benutzereingabe erforderlich. Der Datenträger wird bei Neustart des Computers verschlüsselt.
- TPM + PIN/Kennwort. Bei Vorhandensein des TPM-Moduls erscheint ein Abfragefenster für den PIN-Code. Wenn kein TPM-Modul vorhanden ist, erscheint ein Abfragefenster für das Kennwort für die Preboot-Authentifizierung.
- Nur Kennwort. Es erscheint ein Abfragefenster für das Kennwort für die Preboot-Authentifizierung.

Ist im Betriebssystem der FIPS-Kompatibilitätsmodus (Federal Information Processing Standard) aktiviert, so erscheint in den Betriebssystemen Windows 8 und in älteren Versionen ein Abfragefenster zur Verbindung eines Massenspeichergerätes für die Speicherung der Wiederherstellungsschlüsseldatei. Sie können auf einem Speichergerät mehrere Dateien mit Wiederherstellungsschlüsseln speichern.

Nachdem Sie ein Kennwort oder einen PIN-Code festgelegt haben, fordert BitLocker Sie auf, den Computer neu zu starten, um die Laufwerkverschlüsselung abzuschließen. Anschließend muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach erfolgreichem BitLocker-Authentifizierungsvorgang ist die Anmeldung am System erforderlich. Nach dem Start des Betriebssystems schließt BitLocker die Laufwerkverschlüsselung ab.

Besteht kein Zugriff auf die Chiffrierschlüssel, so kann der Benutzer beim Administrator des lokalen Unternehmensnetzwerks einen Wiederherstellungsschlüssel anfordern (falls zuvor kein Wiederherstellungsschlüssel auf dem Massenspeichergerät gespeichert wurde oder falls er verloren gegangen ist).

Einstellungen der Komponente „BitLocker-Laufwerkverschlüsselung"

Einstellung	Beschreibung
Verwendung der BitLocker-Authentifizierung aktivieren, die Preboot-Tastatureingaben auf Tablets erfordert	Das Kontrollkästchen aktiviert/deaktiviert die Verwendung der Authentifizierung, bei der eine Preboot-Tastatureingabe erforderlich ist, selbst dann, wenn die Plattform keine Option zur Preboot-Eingabe bietet (beispielsweise bei berührungsempfindlichen Tastaturen auf Tablets). Das Touchpad von Tablets ist in der Preboot-Umgebung nicht verfügbar. Um die BitLocker-Authentifizierung auf Tablets auszuführen, muss der Benutzer beispielsweise eine USB-Tastatur anschließen. Ist das Kontrollkästchen aktiviert, so wird die Verwendung der Authentifizierung erlaubt, wenn sie eine Preboot-Tastatureingabe erfordert. Es wird empfohlen, diese Einstellung nur für Geräte zu verwenden, die während des Preboot-Vorgangs außer berührungsempfindlichen Tastaturen auch Alternativen für die Dateneingabe bieten, wie beispielsweise eine USB-Tastatur. Wenn das Kontrollkästchen deaktiviert ist, ist die BitLocker-Laufwerkverschlüsselung auf Tablets nicht möglich.
Hardwareverschlüsselung verwenden (Windows 8 und höhere Versionen)	Ist das Kontrollkästchen aktiviert, so verwendet das Programm die Hardwareverschlüsselung. Dadurch wird erlaubt, die Verschlüsselung zu beschleunigen und die Auslastung der Computerressourcen zu reduzieren.
Nur belegten Speicherplatz verschlüsseln (Windows 8 und höhere Versionen)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt.

	Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Authentifizierungseinstellungen	**Kennwort verwenden (Windows 8 und höhere Versionen)** Bei Auswahl dieser Variante fragt Kaspersky Endpoint Security beim Benutzer das Kennwort ab, wenn auf das verschlüsselte Laufwerk zugegriffen wird. Diese Variante für die Aktion kann gewählt werden, wenn das Trusted Platform Module (TPM) nicht verwendet wird. **Trusted Platform Module (TPM) verwenden** Bei Auswahl dieser Variante verwendet BitLocker das Trusted Platform Module (TPM). *Trusted Platform Module (TPM)* ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten. Für Computer mit den Betriebssystemen Windows 7 und Windows Server 2008 R2 ist nur die Verschlüsselung unter Verwendung eines TPM-Moduls verfügbar. Wenn kein TPM-Modul installiert ist, ist die BitLocker-Verschlüsselung nicht möglich. Die Verwendung eines Kennworts wird auf diesen Computern nicht unterstützt. Ein Gerät, das mit Trusted Platform Module ausgerüstet ist, kann Chiffrierschlüssel erstellen, die nur seiner Hilfe entschlüsselt werden können. Das Trusted Platform Module verschlüsselt Chiffrierschlüssel mit einem eigenen Storage Root Key. Der Storage Root Key wird im Trusted Platform Module aufbewahrt. Dadurch wird für die Chiffrierschlüssel ein zusätzlicher Schutz vor Angriffsversuchen gewährleistet. Diese Aktion ist standardmäßig ausgewählt. Sie können eine zusätzliche Schutzebene für den Zugriff auf den Chiffrierschlüssel einrichten und den Schlüssel mit einem Kennwort oder einer PIN verschlüsseln: • **PIN für TPM verwenden**. Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer einen PIN-Code verwenden, um auf einen Chiffrierschlüssel zuzugreifen, der im Trusted Platform Module (TPM) aufbewahrt wird. Wenn das Kontrollkästchen deaktiviert ist, ist es dem Benutzer verboten, einen PIN-Code zu verwenden. Um Zugriff auf den Chiffrierschlüssel zu erhalten, verwendet der Benutzer ein Kennwort. Sie können dem Benutzer erlauben, eine erweiterte PIN zu verwenden. Eine *erweiterte PIN* ermöglicht neben der Verwendung numerischer Zeichen auch lateinische Groß- und Kleinbuchstaben, Sonderzeichen und Leerzeichen.

	• **Trusted Platform Module (TPM) verwenden; falls nicht verfügbar, Kennwort verwenden**. Ist das Kontrollkästchen aktiviert, so kann der Benutzer beim Fehlen des Trusted Platform Module (TPM) mithilfe des Kennworts Zugriff auf die Chiffrierschlüssel erhalten. Wenn das Kontrollkästchen deaktiviert ist und das TPM-Modus nicht verfügbar ist, wird die vollständige Festplattenverschlüsselung nicht gestartet.

Entschlüsselung einer Festplatte, die mit BitLocker geschützt ist

Der Benutzer kann das Laufwerk selbstständig mithilfe von Betriebssystem-Tools entschlüsseln (Funktion *BitLocker deaktivieren*). Anschließend schlägt Kaspersky Endpoint Security vor, das Laufwerk erneut zu verschlüsseln. Kaspersky Endpoint Security schlägt so lange vor, das Laufwerk zu verschlüsseln, bis Sie die Entschlüsselung von Laufwerken in der Richtlinie aktivieren.

So entschlüsseln Sie eine durch BitLocker geschützte Festplatte über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Element **BitLocker-Laufwerkverschlüsselung** aus.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Alle Festplatten entschlüsseln** aus.
8. Speichern Sie die vorgenommenen Änderungen.

So entschlüsseln Sie eine mit BitLocker verschlüsselte Festplatte über die Web Console und die Cloud Console

1. Wählen Sie im Hauptfenster der Web Console die Registerkarte **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie für Kaspersky Endpoint Security für jene Computer, auf denen Sie Festplatten entschlüsseln möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **BitLocker-Laufwerkverschlüsselung** aus und klicken Sie auf den Link, um zu den Einstellungen zu wechseln.

   Die Verschlüsselungseinstellungen werden geöffnet.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Alle Festplatten entschlüsseln** aus.
7. Klicken Sie auf **OK**.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool "Encryption Monitor" kann über das Programmhauptfenster ausgeführt werden.

Wiederherstellen des Zugriffs auf einen Datenträger, der mit BitLocker geschützt ist

Wenn der Benutzer das Kennwort für den Zugriff auf eine Festplatte vergessen hat, die mit BitLocker verschlüsselt ist, muss ein Wiederherstellungsvorgang (“Anfrage-Frage“) ausgeführt werden.

Für die Betriebssysteme Windows 8 und für ältere Versionen gilt: Wenn im Betriebssystem der Kompatibilitätsmodus für den Federal Information Processing Standard (FIPS) aktiviert ist, wurde die Wiederherstellungsschlüssel-Datei vor der Verschlüsselung auf dem Wechseldatenträger gespeichert. Um den Zugriff auf den Datenträger wiederherzustellen, verbinden Sie den Datenträger und folgen Sie den Anweisungen auf dem Bildschirm.

Um den Zugriff auf eine Festplatte wiederherzustellen, die mit BitLocker verschlüsselt ist, sind die folgenden Schritte erforderlich:

1. Der Benutzer übermittelt die Wiederherstellungsschlüssel-ID an den Administrator (s. Abb. unten).
2. Der Administrator überprüft die Wiederherstellungsschlüssel-ID in den Computereigenschaften in Kaspersky Security Center. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereigenschaften angezeigt wird.
3. Wenn die IDs der Wiederherstellungsschlüssel übereinstimmen, teilt der Administrator dem Benutzer den Wiederherstellungsschlüssel mit oder übermittelt eine Wiederherstellungsschlüssel-Datei.

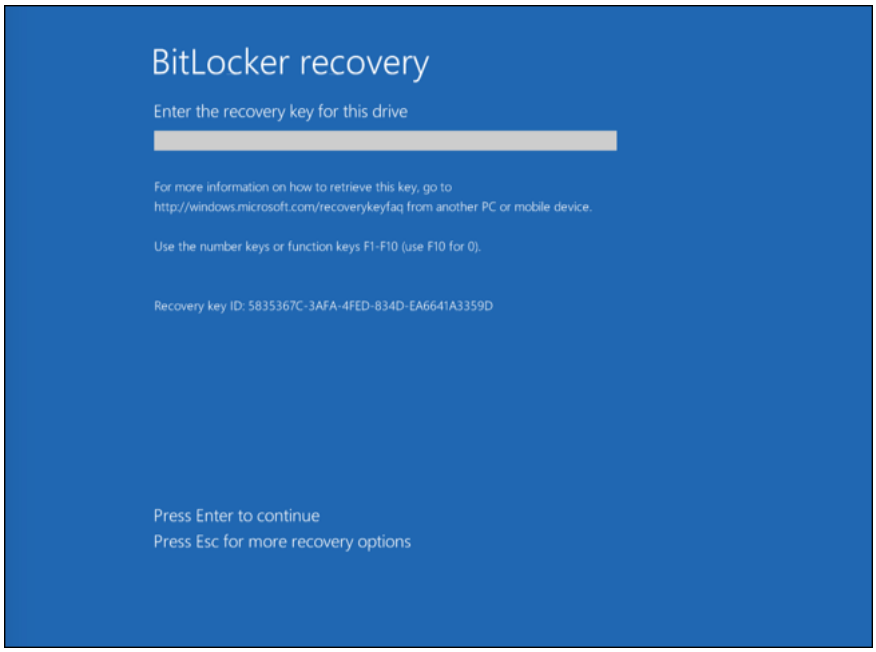
   Eine Wiederherstellungsschlüssel-Datei wird für Computer mit folgenden Betriebssystemen verwendet:

   - Windows 7

- Windows 8
- Windows Server 2008
- Windows Server 2011
- Windows Server 2012

Für die übrigen Betriebssysteme wird ein Wiederherstellungsschlüssel benutzt.

4. Der Benutzer gibt den Wiederherstellungsschlüssel ein und erhält Zugriff auf die Festplatte.



Wiederherstellen des Zugriffs auf eine Festplatte, die mit BitLocker verschlüsselt ist

Wiederherstellen des Zugriffs auf ein Systemlaufwerk

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer während der Preboot-Authentifizierung die Taste **Esc** drücken.

[In der Verwaltungskonsole (MMC) den Wiederherstellungsschlüssel für ein Systemlaufwerk anzeigen, das mit BitLocker verschlüsselt ist]

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der die Wiederherstellung des Zugriffs auf verschlüsselte Daten anfordert, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Zugriff auf ein Systemlaufwerk mit BitLocker-Schutz** aus.
7. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.

[So zeigen Sie in der Web Console und der Cloud Console den Wiederherstellungsschlüssel für ein Systemlaufwerk an, das mit BitLocker verschlüsselt ist]

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte** → **Verwaltete Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.
4. Wählen Sie im folgenden Fenster den Abschnitt **BitLocker** aus.
5. Überprüfen Sie die ID des Wiederherstellungsschlüssels. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereinstellungen angezeigt wird.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.
6. Klicken Sie auf die Schaltfläche **Schlüssel anfordern**.

Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.

Nachdem das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer auf, das Kennwort oder den PIN-Code zu ändern. Nachdem Sie ein neues Kennwort oder einen neuen PIN-Code festgelegt haben, erstellt BitLocker einen neuen Hauptschlüssel und sendet den Schlüssel an das Kaspersky Security Center. Infolgedessen werden der Wiederherstellungsschlüssel und die Wiederherstellungsschlüsseldatei aktualisiert. Wenn der Benutzer das Kennwort nicht geändert hat, können Sie beim nächsten Start des Betriebssystems den alten Wiederherstellungsschlüssel verwenden.

Auf Computern mit Windows 7 kann das Kennwort oder der PIN-Code nicht geändert werden. Nachdem der Wiederherstellungsschlüssel eingegeben wurde und das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer nicht auf, das Kennwort oder den PIN-Code zu ändern. Daher ist es nicht möglich, ein neues Passwort oder einen neuen PIN-Code festzulegen. Dieses Problem beruht auf Besonderheiten des Betriebssystems. Um fortzufahren, müssen Sie die Festplatte neu verschlüsseln.

Wiederherstellen des Zugriffs auf ein Nicht-Systemlaufwerk

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer im Zugriffserteilungsfenster für den Datenträger auf den Link **Kennwort vergessen** klicken. Nachdem der Zugriff auf den verschlüsselten Datenträger gewährt wurde, kann der Benutzer in den BitLocker-Einstellungen festlegen, dass der Datenträger bei der Windows-Authentifizierung automatisch entsperrt wird.

In der Verwaltungskonsole (MMC) den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk anzeigen, das mit BitLocker verschlüsselt ist

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Geräte**.
3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät aus, für das Sie eine Zugriffsschlüsseldatei erstellen möchten, und wählen Sie den Punkt **Zugriff auf das Gerät anfordern bei Kaspersky Endpoint Security für Windows (11.6.0)** aus.
4. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf den angegebenen Datenträger wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.
5. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

So zeigen Sie in der Web Console und der Cloud Console den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk an, das mit BitLocker verschlüsselt ist

1. Wählen Sie im Hauptfenster der „Web Console“ **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.

   Der Assistent für die Zugriffserteilung auf das Gerät wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten für die Zugriffserteilung auf das Gerät:

   a. Wählen Sie das Plug-in für **Kaspersky Endpoint Security für Windows** aus.

   b. Überprüfen Sie die ID des Wiederherstellungsschlüssels. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereinstellungen angezeigt wird.

   > Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

   c. Klicken Sie auf die Schaltfläche **Schlüssel anfordern**.

Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.

Dateiverschlüsselung auf lokalen Festplatten des Computers

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Kaspersky Endpoint Security verschlüsselt/entschlüsselt die Standardordner nur für die lokalen Benutzerprofile (local user profiles) des Betriebssystems. Kaspersky Endpoint Security verschlüsselt und entschlüsselt die Standardordner nicht für Roaming-Benutzerprofile (roaming user profiles), verbindliche Benutzerprofile (mandatory user profiles), temporäre Benutzerprofile (temporary user profiles) und Ordnerumleitung.
- Für Dateien, deren Veränderung die Funktionsfähigkeit des Betriebssystems und der installierten Programme beeinträchtigen kann, führt Kaspersky Endpoint Security keine Verschlüsselung durch. Zur Liste der Verschlüsselungsausnahmen gehören beispielsweise folgende Dateien und Ordner mit allen untergeordneten Ordnern:
  - %WINDIR%
  - %PROGRAMFILES% und %PROGRAMFILES(X86)%

- Dateien der Systemregistrierung von Windows

Die Liste mit Ausnahmen von der Verschlüsselung kann nicht angezeigt oder geändert werden. Dateien und Ordner aus der Liste mit den Verschlüsselungsausnahmen können zur Verschlüsselungsliste hinzugefügt werden; sie werden jedoch bei der Ausführung der Dateiverschlüsselung nicht verschlüsselt.

Dateiverschlüsselung auf lokalen Festplatten des Computers starten

Kaspersky Endpoint Security verschlüsselt die Dateien, deren Inhalt sich in einem OneDrive Cloud-Speicher befindet, nicht und blockiert das Kopieren verschlüsselter Dateien in einen OneDrive Cloud-Speicher, wenn diese Dateien nicht zu einer Entschlüsselungsregel hinzugefügt wurden.

Gehen Sie wie folgt vor, um Dateien auf lokalen Festplatten des Computers zu verschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Dateien verschlüsseln** aus.
6. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Verschlüsselung**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.
8. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:

   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Verschlüsselungsregel hinzuzufügen.

      - **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner.
      - **Favoriten**. Dateien im Standardordner *Favoriten* des Betriebssystems, sowie untergeordnete Ordner.
      - **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner.
      - **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Sicherungskopien von Dokumenten.
      - **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB).

   b. Wählen Sie das Element **Ordnerpfad**, um einen Ordner, dessen Pfad manuell angegeben wird, zur Verschlüsselungsregel hinzuzufügen.

Beachten Sie folgende Regeln, wenn Sie einen Ordnerpfad hinzufügen:

- Verwenden Sie eine Umgebungsvariable (z. B. `%FOLDER%\UserFolder\`). Eine Umgebungsvariable kann nur ein Mal und nur am Anfang des Pfads verwendet werden.
- Verwenden Sie keine relativen Pfade. Sie können einen Satz verwenden `\..\` (z. B. `C:\Users\..\UserFolder\`). Der Satz `\..\` bedeutet einen Wechsel zum übergeordneten Ordner.
- Verwenden Sie nicht die Zeichen `*` und `?`.
- Verwenden Sie keine UNC-Pfade.
- Verwenden Sie `;` oder `,` als Trennzeichen.

c. Wählen Sie das Element **Dateien nach Erweiterung** aus, um bestimmte Dateierweiterungen zu der Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den angegebenen Erweiterungen auf allen lokalen Festplatten des Computers.

d. Wählen Sie das Element **Dateien nach Erweiterungsgruppen** aus, um Gruppen für Dateierweiterungen (z. B. die Gruppe *Microsoft-Office-Dokumente*) zu der Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, auf allen lokalen Festplatten des Computers.

9. Speichern Sie die vorgenommenen Änderungen.

Sofort nachdem die Richtlinie übernommen wurde, verschlüsselt Kaspersky Endpoint Security jene Dateien, die in der Verschlüsselungsregel angegeben sind und nicht in der Entschlüsselungsregel angegeben sind.

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Wenn dieselbe Datei sowohl zu einer Verschlüsselungsregel als auch zu einer Entschlüsselungsregel hinzugefügt wurde, verfährt Kaspersky Endpoint Security wie folgt:
  - Wenn die Quelldatei nicht verschlüsselt ist, verschlüsselt Kaspersky Endpoint Security diese Datei nicht.
  - Wenn die Quelldatei verschlüsselt ist, entschlüsselt Kaspersky Endpoint Security diese Datei.
- Kaspersky Endpoint Security verschlüsselt weiterhin neue Dateien, wenn die Dateien die Kriterien der Verschlüsselungsregel erfüllen. Sie haben beispielsweise die Eigenschaften einer nicht verschlüsselten Datei (Pfad oder Erweiterung) geändert und die Datei erfüllt nun die Kriterien der Verschlüsselungsregel. Kaspersky Endpoint Security verschlüsselt diese Datei.
- Erstellt der Benutzer eine neue Datei, deren Eigenschaften die Kriterien der Verschlüsselungsregel erfüllen, so verschlüsselt Kaspersky Endpoint Security die Datei sofort, wenn die Datei geöffnet wird.
- Kaspersky Endpoint Security wartet mit der Verschlüsselung geöffneter Dateien, bis sie geschlossen werden.
- Wenn Sie eine verschlüsselte Datei in einen anderen Ordner des lokalen Laufwerks verschieben, bleibt die Datei verschlüsselt, unabhängig davon, ob dieser Ordner zur Verschlüsselungsregel gehört.
- Wenn Sie eine Datei entschlüsselt und die Datei in einen anderen Ordner auf einem lokalen Laufwerk kopiert haben, das nicht zur Entschlüsselungsregel gehört, so kann die Dateikopie verschlüsselt werden. Um die Verschlüsselung der Dateikopie zu verhindern, erstellen Sie für den Zielordner eine Entschlüsselungsregel.

Programmzugriffsrechte für verschlüsselte Dateien formulieren

Gehen Sie wie folgt vor, um Programmzugriffsrechte für verschlüsselte Dateien zu formulieren:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Dateien verschlüsseln** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

   Zugriffsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie nach dem Übernehmen von Zugriffsregeln im Modus **Gemäß den Regeln** in den Modus **Nicht verändern** wechseln, so ignoriert Kaspersky Endpoint Security alle Zugriffsregeln. Alle Programme besitzen Zugriff auf alle verschlüsselten Dateien.

7. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.
8. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.
   a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu Werte für die Einstellungen **Programm**, **Hersteller**, **Hinzugefügt** sowie für die Kontrollkästchen aus dem Block **Gruppe** an.
   b. Klicken Sie auf **Aktualisieren**.
   c. In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.
   d. Aktivieren Sie in der Spalte **Programme** die Kontrollkästchen der Programme, für die Sie Zugriffsregeln für verschlüsselte Dateien erstellen möchten.
   e. Wählen Sie in der Dropdown-Liste **Regel für Programme** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.
   f. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Zugriffsregeln für verschlüsselte Dateien ausführen soll, die bereits für die oben angegebenen Programme vorhanden sind.
   g. Klicken Sie auf **OK**.

   Die Informationen zur Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle in der Registerkarte **Regeln für Programme** angezeigt.
9. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

   Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

c. Wählen Sie in der Dropdown-Liste **Regel für Programme** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.

d. Klicken Sie auf **OK**.

Die Informationen zur Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle in der Registerkarte **Regeln für Programme** angezeigt.

10. Speichern Sie die vorgenommenen Änderungen.

Verschlüsselung von Dateien, die von bestimmten Programmen erstellt und geändert werden

Sie können eine Regel erstellen, nach der Kaspersky Endpoint Security alle Dateien verschlüsseln soll, welche von in der Regel angegebenen Programmen erstellt oder geändert werden.

> Dateien, die von den angegebenen Programmen erstellt oder geändert worden sind, bevor die Verschlüsselungsregel übernommen wurde, werden nicht verschlüsselt.

Um die Verschlüsselung von Dateien anzupassen, die von bestimmten Programmen erstellt und geändert werden, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Dateien verschlüsseln** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

   > Verschlüsselungsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie nach dem Übernehmen von Verschlüsselungsregeln im Modus **Gemäß den Regeln** in den Modus **Nicht verändern** wechseln, so ignoriert Kaspersky Endpoint Security alle Verschlüsselungsregeln. Dateien, die zuvor verschlüsselt worden sind, bleiben weiterhin verschlüsselt.

7. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.

8. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.

   Das Fenster **Programme aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

   Gehen Sie wie folgt vor:

   a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu Werte für die Einstellungen **Programm**, **Hersteller**, **Hinzugefügt** sowie für die Kontrollkästchen aus dem Block **Gruppe** an.

   b. Klicken Sie auf **Aktualisieren**.

      In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.

   c. Aktivieren Sie in der Spalte **Programme** die Kontrollkästchen jener Programme, deren erstellte Dateien Sie verschlüsseln möchten.

   d. Wählen Sie in der Liste **Regel für Programme** das Element **Alle neu erstellten Dateien verschlüsseln**.

   e. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Verschlüsselungsregeln für Dateien ausführen soll, die bereits für die oben angegebenen Programme erstellt worden sind.

   f. Klicken Sie auf **OK**.

   Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Programmen erstellt und geändert wurden, werden in einer Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

9. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

   Das Fenster **Namen von ausführbaren Programmdateien hinzufügen / ändern** wird geöffnet.

   Gehen Sie wie folgt vor:

   a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

      Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

   b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

   c. Wählen Sie in der Liste **Regel für Programme** das Element **Alle neu erstellten Dateien verschlüsseln**.

   d. Klicken Sie auf **OK**.

   Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Programmen erstellt und geändert wurden, werden in einer Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

10. Speichern Sie die vorgenommenen Änderungen.

Entschlüsselungsregel erstellen

Um eine Entschlüsselungsregel zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Dateien verschlüsseln** aus.

6. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Entschlüsselung**.

7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

8. Klicken Sie auf der Registerkarte **Entschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:

   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Entschlüsselungsregel hinzuzufügen.

   b. Wählen Sie das Element **Ordnerpfad**, um den Ordner, dessen Pfad manuell angegeben wird, zur Entschlüsselungsregel hinzuzufügen.

   c. Wählen Sie das Element **Dateien nach Erweiterung** aus, um bestimmte Dateierweiterungen zu der Entschlüsselungsregel hinzuzufügen. Dateien mit den angegebenen Erweiterungen werden auf allen lokalen Festplatten des Computers nicht von Kaspersky Endpoint Security verschlüsselt.

   d. Wählen Sie das Element **Dateien nach Erweiterungsgruppen** aus, um Gruppen für Dateierweiterungen (z. B. die Gruppe *Microsoft-Office-Dokumente*) zu der Entschlüsselungsregel hinzuzufügen. Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, werden von Kaspersky Endpoint Security auf allen lokalen Festplatten des Computers nicht verschlüsselt.

9. Speichern Sie die vorgenommenen Änderungen.

Wurde eine Datei sowohl zur Verschlüsselungsregel als auch zur Entschlüsselungsregel hinzugefügt, so geht Kaspersky Endpoint Security wie folgt vor: Wenn die Datei nicht verschlüsselt ist, wird sie nicht verschlüsselt, und wenn die Datei verschlüsselt ist, wird sie entschlüsselt.

Dateientschlüsselung auf lokalen Festplatten des Computers

Gehen Sie wie folgt vor, um Dateien auf lokalen Datenträgern des Computers zu entschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Dateien verschlüsseln** aus.

6. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Verschlüsselung**.

7. Schließen Sie aus der Verschlüsselungsliste alle Dateien und Ordner aus, die Sie entschlüsseln möchten. Wählen Sie dazu in der Liste diese Dateien aus und wählen Sie im Kontextmenü der Schaltfläche **Löschen** den Punkt **Regel löschen und Dateien entschlüsseln**.

   Sie können mehrere Elemente gleichzeitig aus der Verschlüsselungsliste löschen. Halten Sie dazu die Taste **STRG** gedrückt, während Sie mit der linken Maustaste die entsprechenden Elemente auswählen. Wählen Sie dann im Kontextmenü der Schaltfläche **Löschen** den Punkt **Regel löschen und Dateien entschlüsseln** aus.

   Die aus der Verschlüsselungsliste gelöschten Dateien und Ordner werden automatisch zur Entschlüsselungsliste hinzugefügt.

8. Erstellen Sie eine Dateiliste für Entschlüsselung

9. Speichern Sie die vorgenommenen Änderungen.

Unmittelbar nach der Übernahme der Richtlinie entschlüsselt Kaspersky Endpoint Security die verschlüsselten Dateien, die der Entschlüsselungsliste hinzugefügt wurden.

Kaspersky Endpoint Security entschlüsselt verschlüsselte Dateien, wenn ihre Parameter (Dateipfad / Dateiname / Dateierweiterung) geändert wurden und nach der Änderung den Parametern der Objekte entsprechen, die in die Entschlüsselungsliste aufgenommen sind.

Kaspersky Endpoint Security wartet mit der Entschlüsselung geöffneter Dateien, bis sie geschlossen werden.

Verschlüsselte Archive erstellen

Für den Schutz von Daten, die von Benutzern innerhalb des Unternehmensnetzwerks mit Dateien übertragen werden, können Sie verschlüsselte Archive verwenden. Verschlüsselte Archive eignen sich zur Übertragung großer Dateien mithilfe von Wechseldatenträgern, da E-Mail-Clients eine Größenbeschränkung für Dateien haben.

Vor dem Erstellen eines verschlüsselten Archivs fragt Kaspersky Endpoint Security den Benutzer nach einem Kennwort. Um einen zuverlässigen Datenschutz zu gewährleisten, können Sie die Überprüfung der Kennwortstärke aktivieren und Komplexitätskriterien festlegen. In diesem Fall ist die Verwendung kurzer und einfacher Kennwörter untersagt (wie beispielsweise `1234`).

Aktivieren der Kennwortstärkeprüfung beim Erstellen verschlüsselter Archive in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Allgemeine Verschlüsselungseinstellungen** aus.
6. Klicken Sie im Block **Einstellungen für Kennwörter** auf die Schaltfläche **Einstellungen**.
7. Wählen Sie im folgenden Fenster die Registerkarte **Verschlüsselte Archive** aus.
8. Passen Sie die Einstellungen für die Kennwortstärke an, die beim Erstellen verschlüsselter Archive gelten sollen.

[So aktivieren Sie die Kennwortstärkeprüfung beim Erstellen verschlüsselter Archive in der Web Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Überprüfung der Kennwortstärke aktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Datenverschlüsselung → Dateien verschlüsseln**.
5. Konfigurieren Sie im Block **Einstellungen für Kennwörter für verschlüsselte Archive** die Kriterien für die Kennwortstärke, die beim Erstellen verschlüsselter Archive gelten sollen.

Verschlüsselte Archive können Sie auf Computern erstellen, auf denen das Programm Kaspersky Endpoint Security mit der Funktion zur Datenverschlüsselung installiert ist.

Wenn zu einem verschlüsselten Archiv eine Datei hinzugefügt wird, deren Inhalt sich im Cloud-Speicher OneDrive befindet, lädt Kaspersky Endpoint Security den Inhalt der entsprechenden Datei herunter und führt die Verschlüsselung aus.

Gehen Sie folgendermaßen vor, um ein verschlüsseltes Archiv zu erstellen:

1. Verwenden Sie einen beliebigen Dateimanager, um die Dateien und Ordner zu markieren, die Sie zu einem verschlüsselten Archiv hinzufügen möchten. Öffnen Sie durch Rechtsklick das Kontextmenü.
2. Wählen Sie im Kontextmenü den Punkt **Verschlüsseltes Archiv erstellen** aus (s. Abb. unten).

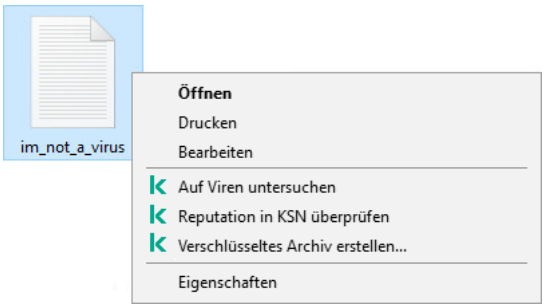
3. Geben Sie im folgenden Fenster an, wo das verschlüsselte Archiv auf dem Wechseldatenträger gespeichert werden soll, legen Sie einen Namen fest und klicken Sie auf **Speichern**.

4. Legen Sie im folgenden Fenster ein Kennwort fest und bestätigen Sie es.

   Das Kennwort muss den Komplexitätskriterien entsprechen, die in der Richtlinie angegeben sind.

5. Klicken Sie auf **Erstellen**.

Der Vorgang zur Erstellung eines verschlüsselten Archivs wird gestartet. Während der Erstellung eines verschlüsselten Archivs nimmt Kaspersky Endpoint Security keine Dateikomprimierung vor. Nach Abschluss des Vorgangs wird am angegebenen Speicherort auf dem Datenträger ein selbstentpackendes Archiv erstellt, das verschlüsselt und durch ein Kennwort geschützt ist (ausführbare Datei mit der Erweiterung exe) – .



Verschlüsseltes Archiv erstellen

Um Zugriff auf die Dateien in einem verschlüsselten Archiv zu erhalten, muss der Assistent zum Extrahieren des Archivs gestartet werden. Der Assistent wird durch Doppelklick und Kennworteingabe gestartet. Wenn Sie das Kennwort vergessen haben, kann der Zugriff auf die Dateien in einem verschlüsselten Archiv nicht wiederhergestellt werden. Sie können ein neues verschlüsseltes Archiv erstellen.

Wiederherstellen des Zugriffs auf verschlüsselte Dateien

Bei der Dateiverschlüsselung erhält Kaspersky Endpoint Security einen Chiffrierschlüssel, der für den direkten Zugriff auf die verschlüsselten Dateien erforderlich ist. Mithilfe eines Chiffrierschlüssels kann ein Benutzer direkten Zugriff auf verschlüsselte Dateien erhalten. Voraussetzung dafür ist, dass der Benutzer bei einem beliebigen Windows-Benutzerkonto angemeldet ist, das zum Zeitpunkt der Dateiverschlüsselung aktiv war. Damit Benutzer, die bei Windows-Benutzerkonten angemeldet sind, welche zum Zeitpunkt der Dateiverschlüsselung inaktiv waren, auf verschlüsselte Dateien zugreifen können, ist eine Verbindung mit Kaspersky Security Center erforderlich.

Verschlüsselte Dateien können in folgenden Fällen nicht verfügbar sein:

- Auf dem Benutzercomputer sind Chiffrierschlüssel vorhanden, es besteht aber keine Verbindung zu Kaspersky Security Center. Diese Verbindung ist für die Arbeit mit Chiffrierschlüsseln erforderlich. In diesem Fall muss der Benutzer den Zugriff auf die verschlüsselten Dateien beim Administrator des lokalen Unternehmensnetzwerks anfordern.

  Wenn keine Verbindung zu Kaspersky Security Center besteht, ist es erforderlich:

  - für den Zugriff auf verschlüsselte Dateien, die auf Computerfestplatten gespeichert sind, einen Zugriffsschlüssel anzufordern
  - für den Zugriff auf verschlüsselte Dateien, die auf Wechseldatenträgern gespeichert sind, für jeden Wechseldatenträger einen separaten Zugriffsschlüssel für die verschlüsselten Dateien anzufordern.

- Die Verschlüsselungskomponenten wurden vom Benutzercomputer entfernt. In diesem Fall kann der Benutzer verschlüsselte Dateien auf lokalen Datenträgern und auf Wechseldatenträgern zwar öffnen, der Inhalt der Dateien wird aber in verschlüsselter Form angezeigt.

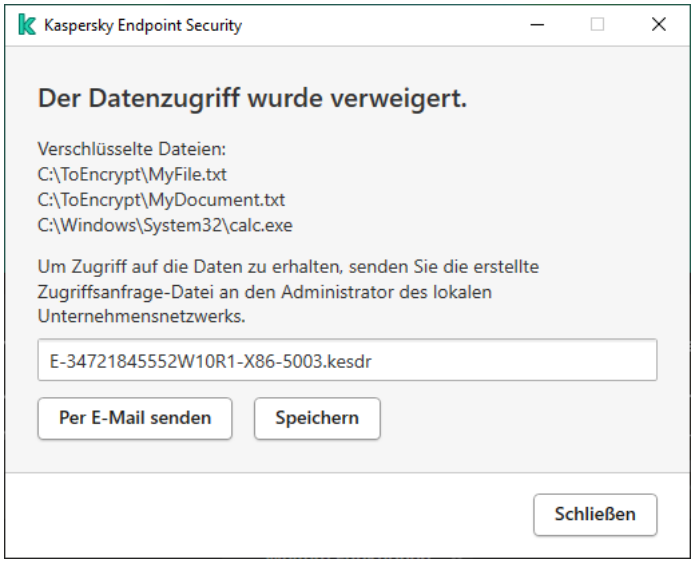
Der Benutzer kann unter folgenden Bedingungen mit verschlüsselten Dateien arbeiten:

- Die Dateien befinden sich in verschlüsselten Archiven, die auf einem Computer erstellt wurden, auf dem das Programm Kaspersky Endpoint Security installiert ist.
- Die Dateien sind auf Wechseldatenträgern gespeichert, für welche die Arbeit im portablen Modus zugelassen ist.

Um Zugriff auf die verschlüsselten Dateien zu erhalten, muss der Benutzer den Wiederherstellungsvorgang ("Anfrage-Frage") starten.

Der Zugriff auf die verschlüsselten Dateien wird mit den folgenden Schritten wiederhergestellt:

1. Der Benutzer sendet eine Zugriffsanfrage-Datei an den Administrator (s. Abb. unten).
2. Der Administrator fügt die Zugriffsanfrage-Datei in Kaspersky Security Center hinzu, erstellt eine Zugriffsschlüsseldatei und sendet diese Datei an den Benutzer.
3. Der Benutzer fügt die Zugriffsschlüsseldatei in Kaspersky Endpoint Security hinzu und erhält Zugriff auf die Dateien.



Wiederherstellen des Zugriffs auf verschlüsselte Dateien

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf eine Datei zugreifen. Dann erstellt Kaspersky Endpoint Security eine Zugriffsanfrage-Datei (Datei mit der Erweiterung kesdc), die beispielsweise per E-Mail an den Administrator übermittelt werden muss.

Kaspersky Endpoint Security erstellt eine Zugriffsanfrage-Datei, die für alle verschlüsselten Dateien gilt, die auf dem Computerlaufwerk (lokales Laufwerk oder Wechseldatenträger) gespeichert sind.

In der Verwaltungskonsole (MMC) eine Zugriffsschlüsseldatei für verschlüsselte Daten anfordern

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der die Wiederherstellung des Zugriffs auf verschlüsselte Daten anfordert, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Datenverschlüsselung** aus.
7. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.
8. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.

In der „Web Console“ eine Zugriffsschlüsseldatei für verschlüsselte Daten anfordern

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Verwaltete Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.
4. Wählen Sie den Abschnitt **Datenverschlüsselung** aus.
5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.
6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Nachdem der Benutzer die Zugriffsschlüsseldatei für die verschlüsselten Daten erhalten hat, muss er die Datei durch Doppelklick starten. Dann gewährt Kaspersky Endpoint Security den Zugriff auf alle verschlüsselten Dateien, die auf dem Laufwerk gespeichert sind. Um Zugriff auf verschlüsselte Dateien zu erhalten, die sich auf anderen Datenträgern befinden, müssen separate Zugriffsschlüssel für diese Datenträger angefordert werden.

Zugriff auf verschlüsselte Daten beim Ausfall des Betriebssystems wiederherstellen

Wenn das Betriebssystem ausfällt, ist die Wiederherstellung des Datenzugriffs nur für die Dateiverschlüsselung (FLE) verfügbar. Bei der vollständigen Festplattenverschlüsselung (FDE) ist es nicht möglich, den Datenzugriff wiederherzustellen.

Um bei einem Ausfall des Betriebssystems den Zugriff auf verschlüsselte Daten wiederherzustellen, gehen Sie wie folgt vor:

1. Installieren Sie das Betriebssystem neu, ohne die Festplatte zu formatieren.
2. Installieren Sie Kaspersky Endpoint Security.
3. Stellen Sie eine Verbindung zwischen dem Computer und dem Administrationsserver für Kaspersky Security Center her, von dem der Computer während der Datenverschlüsselung verwaltet wurde.

Der Zugriff auf verschlüsselte Daten wird zu den gleichen Bedingungen gewährt, wie sie vor dem Ausfall des Betriebssystems galten.

Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anpassen

Gehen Sie wie folgt vor, um Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anzupassen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Allgemeine Verschlüsselungseinstellungen** aus.
6. Klicken Sie im Abschnitt **Vorlagen** auf **Vorlagen**.

   Das Fenster **Vorlagen** wird geöffnet.
7. Gehen Sie wie folgt vor:

   - Um die Vorlage für eine vom Benutzer gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Benutzer**. Greift der Benutzer auf eine verschlüsselte Datei zu, wenn sich auf dem Computer kein Zugriffsschlüssel für die verschlüsselten Dateien befindet, so wird das Fenster **Der Datenzugriff wurde verweigert** geöffnet. Bei Klick auf **Per E-Mail senden** im Fenster **Der Datenzugriff wurde verweigert** wird automatisch eine vom Benutzer stammende Nachricht erstellt. Diese Nachricht wird zusammen mit der Anforderungsdatei für den Zugriff auf verschlüsselte Dateien an den Administrator des lokalen Unternehmensnetzwerks gesendet.

- Um die Vorlage für eine vom Administrator gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Administrator**. Diese Nachricht wird durch Klick auf **Per E-Mail senden** im Fenster **Anfrage für den Zugriff auf verschlüsselte Dateien** automatisch erstellt und an den Benutzer zugestellt, nachdem ihm der Zugriff auf verschlüsselte Dateien gewährt wurde.

8. Ändern Sie die Meldungsvorlagen.

   Sie können die Schaltfläche **Standard** und die Dropdown-Liste **Variable** verwenden.

9. Speichern Sie die vorgenommenen Änderungen.

Wechseldatenträger verschlüsseln

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Kaspersky Endpoint Security unterstützt die Dateiverschlüsselung in FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselung dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus „Nur Lesen“ fest.

Um die Daten auf Wechseldatenträgern zu schützen, können Sie folgende Verschlüsselungsmethoden verwenden:

- Vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE).

  Verschlüsselung des gesamten Wechseldatenträgers, einschließlich des Dateisystems.

  Es ist nicht möglich, außerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen. Außerdem ist es nicht möglich, innerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen, wenn der Computer nicht mit Kaspersky Security Center (“Gast-Computer“) verbunden ist.

- Verschlüsselung von Dateien (File Level Encryption, FLE).

  Nur Dateien auf dem Wechseldatenträger verschlüsseln. Dabei wird das Dateisystem nicht verändert.

  Die Verschlüsselung von Dateien auf Wechseldatenträgern ermöglicht es, auch außerhalb des Unternehmensnetzwerks auf die Daten zuzugreifen. Dazu dient der *portable Modus*.

Bei der Verschlüsselung erstellt Kaspersky Endpoint Security einen Master-Schlüssel. Kaspersky Endpoint Security speichert den Master-Schlüssel in den folgenden Speichern:

- Kaspersky Security Center.
- Benutzercomputer.

  Der Master-Schlüssel wird mit einem Geheimschlüssel des Benutzers verschlüsselt.

- Wechseldatenträger.

Der Master-Schlüssel wird mit einem offenen Schlüssel von Kaspersky Security Center verschlüsselt.

Nach der Verschlüsselung sind die Daten auf dem Wechseldatenträger innerhalb des Unternehmensnetzwerks verfügbar, als würde ein gewöhnlicher unverschlüsselter Wechseldatenträger verwendet.

Zugriffserteilung auf verschlüsselte Daten

Wenn eine Wechseldatenträger mit verschlüsselten Daten verbunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

1. Es wird überprüft, ob in der lokalen Datenverwaltung auf dem Benutzercomputer ein Master-Schlüssel vorhanden ist.

   Wenn ein Master-Schlüssel gefunden wird, erhält der Benutzer Zugriff auf die Daten des Wechseldatenträgers.

   Wenn kein Master-Schlüssel gefunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

   a. Es wird eine Anfrage an Kaspersky Security Center gesendet.

      Daraufhin sendet Kaspersky Security Center eine Antwort mit einem Master-Schlüssel.

   b. Kaspersky Endpoint Security speichert den Master-Schlüssel in der lokalen Datenverwaltung auf dem Benutzercomputer, um ihn künftig für den verschlüsselten Wechseldatenträger zu verwenden.

2. Die Daten werden entschlüsselt.

Besonderheiten bei der Verschlüsselung von Wechseldatenträgern

Für die Verschlüsselung von Wechseldatenträgern gelten die folgenden Besonderheiten:

- Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Gruppe von verwalteten Computern erstellt. Deshalb ist das Ergebnis, das durch das Übernehmen der Richtlinie für Kaspersky Security Center mit angepasster Verschlüsselung/Entschlüsselung von Wechseldatenträgern erreicht wird, davon abhängig, mit welchen Computern ein Wechseldatenträger verbunden ist.

- Für Dateien mit dem Zugriffsstatus „nur Lesen“, die auf Wechseldatenträgern gespeichert sind, führt Kaspersky Endpoint Security keine Dateiverschlüsselung/-entschlüsselung durch.

- Als Wechseldatenträger werden folgende Gerätetypen unterstützt:

  - Datenträger, die über eine USB-Schnittstelle verbunden werden

  - Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

  - SSD-Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

Verschlüsselung von Wechseldatenträgern starten

Sie können einen Wechseldatenträger mithilfe einer Richtlinie entschlüsseln. Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Administrationsgruppe erstellt. Deshalb hängt das Ergebnis der Datenentschlüsselung auf Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Kaspersky Endpoint Security unterstützt die Verschlüsselung von FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger verbunden wird, der ein nicht unterstütztes Dateisystem hat, so wird die Verschlüsselung des Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger das Zugriffsrecht „nur Lesen“ fest.

Um Wechseldatenträger zu verschlüsseln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Wechseldatenträger verschlüsseln** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion aus, die Kaspersky Endpoint Security standardmäßig mit Wechseldatenträgern ausführen soll:

   - **Gesamten Wechseldatenträger verschlüsseln** (FDE). Kaspersky Endpoint Security verschlüsselt den Inhalt eines Wechseldatenträgers sektorweise. Dabei werden nicht nur die Dateien verschlüsselt, die auf dem Wechseldatenträger gespeichert sind, sondern auch die Dateisysteme, einschließlich Dateinamen und Ordnerstrukturen, auf dem Wechseldatenträger.
   - **Alle Dateien verschlüsseln** (FLE). Kaspersky Endpoint Security verschlüsselt alle Dateien, die auf Wechseldatenträgern gespeichert sind. Nicht verschlüsselt werden die Dateisysteme von Wechseldatenträgern sowie Dateinamen und Ordnerstrukturen.
   - **Nur neue Dateien verschlüsseln** (FLE). Kaspersky Endpoint Security verschlüsselt nur jene Dateien, die zu Wechseldatenträgern hinzugefügt wurden, oder die bereits auf Wechseldatenträgern gespeichert waren und verändert wurden, nachdem die Richtlinie für Kaspersky Security Center zum letzten Mal übernommen wurde.

   Ein bereits verschlüsselter Wechseldatenträger wird durch Kaspersky Endpoint Security nicht erneut verschlüsselt.

7. Wenn Sie den portablen Modus verwenden möchten, um Wechseldatenträger zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Portabler Modus**.

   Der *portable Modus* ist ein Verschlüsselungsmodus für Dateien (FLE) auf Wechseldatenträgern. Der Modus ermöglicht einen Datenzugriff auch außerhalb des Unternehmensnetzwerks. Der portable Modus ermöglicht es außerdem, auf Computern, auf denen das Programm Kaspersky Endpoint Security nicht installiert ist, mit verschlüsselten Dateien zu arbeiten.

8. Wenn Sie einen neuen Wechseldatenträger verschlüsseln möchten, sollten Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln** aktivieren. Ist das Kontrollkästchen deaktiviert, so verschlüsselt Kaspersky Endpoint Security alle Dateien, einschließlich Reste gelöschter oder veränderter Dateien.
9. Um die Verschlüsselung für bestimmte Wechseldatenträger anzupassen, können Sie Verschlüsselungsregeln angeben.

10. Um die vollständige Festplattenverschlüsselung für Wechseldatenträger im Offline-Modus zu verwenden, aktivieren Sie das Kontrollkästchen **Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben**.

    Offline-Verschlüsselungsmodus – Verschlüsselungsmodus für Wechseldatenträger (FDE), wenn keine Verbindung zu Kaspersky Security Center besteht. Bei der Verschlüsselung speichert Kaspersky Endpoint Security den Master-Schlüssel nur auf dem Benutzercomputer. Kaspersky Endpoint Security sendet den Master-Schlüssel bei der nächsten Synchronisierung an Kaspersky Security Center.

    Ist der Computer beschädigt, auf dem der Master-Schlüssel liegt, und die Daten wurden nicht an Kaspersky Security Center gesendet, so ist kein Zugriff auf den Wechseldatenträger möglich.

    Wenn das Kontrollkästchen **Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben** deaktiviert ist und keine Verbindung zu Kaspersky Security Center besteht, kann der Wechseldatenträger nicht verschlüsselt werden.

11. Speichern Sie die vorgenommenen Änderungen.

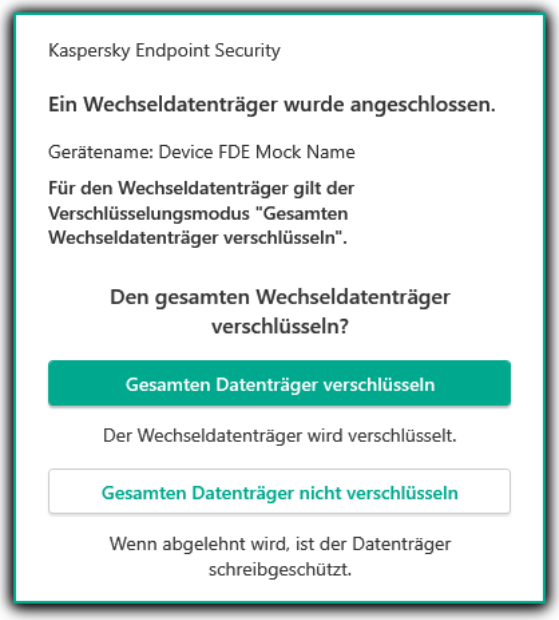
Wenn eine Richtlinie übernommen wurde und der Benutzer einen Wechseldatenträger anschließt oder bereits ein Wechseldatenträger verbunden ist, fragt Kaspersky Endpoint Security nach einer Bestätigung für den Verschlüsselungsvorgang (siehe folgende Abb.).

Das Programm bietet die folgenden Aktionen zur Auswahl:

- Wenn der Benutzer die Verschlüsselungsanfrage bestätigt, verschlüsselt Kaspersky Endpoint Security die Daten.
- Wenn der Benutzer die Verschlüsselungsanfrage ablehnt, verändert Kaspersky Endpoint Security die Daten nicht und legt für diesen Wechseldatenträger das Zugriffsrecht „nur Lesen“ fest.
- Wenn der Benutzer die Verschlüsselungsanfrage nicht beantwortet, verändert Kaspersky Endpoint Security die Daten nicht und legt für diesen Wechseldatenträger das Zugriffsrecht „nur Lesen“ fest. Wenn die Richtlinie zum nächsten Mal angewendet wird oder wenn dieser Wechseldatenträger zum nächsten Mal verbunden wird, fragt das Programm erneut nach einer Bestätigung.

Initiiert der Benutzer während der Datenverschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenverschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Verschlüsselungsvorgangs sicher zu entfernen. Die Datenverschlüsselung wird vorgeschlagen, wenn der Wechseldatenträger zum nächsten Mal mit dem Computer verbunden wird.

Wenn die Verschlüsselung des Wechseldatenträgers fehlgeschlagen ist, überprüfen Sie den Bericht **Virtuelle Datentresore** auf der Benutzeroberfläche von Kaspersky Endpoint Security. Möglicherweise ist der Zugriff auf die Dateien durch ein anderes Programm gesperrt. Versuchen Sie in diesem Fall, den Wechseldatenträger vom Computer zu trennen und erneut zu verbinden.



Anfrage zur Verschlüsselung eines Wechseldatenträgers

Verschlüsselungsregel für Wechseldatenträger hinzufügen

Um eine Verschlüsselungsregel für Wechseldatenträger hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Wechseldatenträger verschlüsseln** aus.
6. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente aus:
   - Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste der vertrauenswürdigen Geräte für die Komponente „Gerätekontrolle“ stehen, wählen Sie das Element **Aus der Liste für vertrauenswürdige Geräte dieser Richtlinie**.
   - Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste für Kaspersky Security Center stehen, wählen Sie das Element **Aus der Liste für Kaspersky Security Center**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** die Aktion aus, die Kaspersky Endpoint Security mit auf Wechseldatenträgern gespeicherten Dateien ausführen soll.
8. Aktivieren Sie das Kontrollkästchen **Portabler Modus**, wenn Kaspersky Endpoint Security die Wechseldatenträger vor der Verschlüsselung so vorbereiten soll, dass die darauf verschlüsselten Dateien im portablen Modus verfügbar sind.

   Im portablen Modus können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

9. Aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**, damit Kaspersky Endpoint Security nur jene Laufwerkssektoren verschlüsselt, die mit Dateien belegt sind.

   Verwenden Sie die Verschlüsselung auf einem Datenträger, der bereits benutzt wurde, so sollte der gesamte Datenträger verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, aus denen noch Informationen entnommen werden können. Die Funktion **Nur belegten Speicherplatz verschlüsseln** wird für neue Datenträger empfohlen, die bisher noch nicht benutzt wurden.

   Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, so werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Gesamten Wechseldatenträger verschlüsseln** übernommen wurde.

10. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Geräte** die Aktion aus, die Kaspersky Endpoint Security mit Verschlüsselungsregeln ausführen soll, die bereits für Wechseldatenträger festgelegt wurden.

    - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger nicht ändern möchten, wählen Sie das Element **Überspringen**.
    - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger durch eine neue Regel ersetzen möchten, wählen Sie das Element **Aktualisieren**.

11. Speichern Sie die vorgenommenen Änderungen.

Die hinzugefügten Verschlüsselungsregeln für Wechseldatenträger werden auf Wechseldatenträger angewendet, die mit einem beliebigen Computer des Unternehmens verbunden sind.

Exportieren und Importieren einer Liste von Verschlüsselungsregeln für Wechseldatenträger

Sie können die Liste der Regeln der Wechseldatenträger-Verschlüsselung in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Wechseldatenträgern desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um die Liste der Regeln zu sichern oder die Regeln auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Regeln für die Verschlüsselung von Wechseldatenträgern in die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Wechseldatenträger verschlüsseln** aus.
6. So exportieren Sie die Liste der Verschlüsselungsregeln für Wechseldatenträger:
   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Klicken Sie auf **Speichern**.
      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
7. So importieren Sie eine Liste von Verschlüsselungsregeln für Wechseldatenträger:
   a. Klicken Sie auf **Import**.
      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.
      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

[So exportieren und importieren Sie eine Liste von Verschlüsselungsregeln für Wechseldatenträger in der Web Console]

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte → Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Kaspersky Endpoint Security-Richtlinie für Computer, auf denen Sie eine Liste von Verschlüsselungsregeln für Wechseldatenträger exportieren oder importieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Virtuelle Datentresore → Verschlüsselung von Wechseldatenträgern**.
5. Klicken Sie im Block **Verschlüsselungsregeln für ausgewählte Geräte** auf den Link **Verschlüsselungsregeln**.

   Dies öffnet eine Liste von Verschlüsselungsregeln für Wechseldatenträger.
6. So exportieren Sie die Liste der Verschlüsselungsregeln für Wechseldatenträger:
   a. Wählen Sie die Regeln, die Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Bestätigen Sie, dass Sie nur die ausgewählten Regeln exportieren möchten, oder exportieren Sie die gesamte Liste.
   d. Klicken Sie auf **Export**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine XML-Datei im Standard-Download-Ordner.
7. So importieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Klicken Sie auf **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Klicken Sie auf **Öffnen**.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

Portabler Modus für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern

Der *portable Modus* ist ein Verschlüsselungsmodus für Dateien (FLE) auf Wechseldatenträgern. Der Modus ermöglicht einen Datenzugriff auch außerhalb des Unternehmensnetzwerks. Der portable Modus ermöglicht es außerdem, auf Computern, auf denen das Programm Kaspersky Endpoint Security nicht installiert ist, mit verschlüsselten Dateien zu arbeiten.

Der portable Modus bietet sich in folgenden Fällen an:

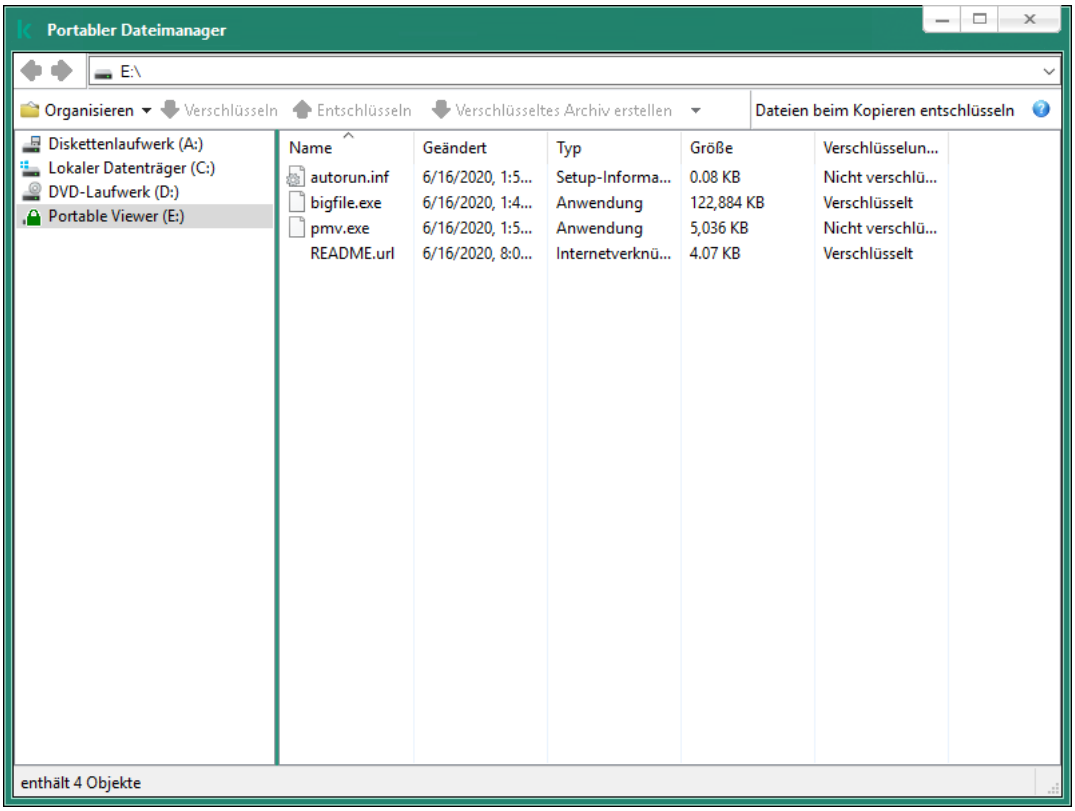
- Es besteht keine Verbindung zwischen dem Computer und dem Kaspersky Security Center Administrationsserver.
- Durch eine Änderung des Kaspersky Security Center Administrationsservers hat sich die Infrastruktur geändert.
- Das Programm Kaspersky Endpoint Security ist nicht auf dem Computer installiert.

Portabler Dateimanager

Für den portablen Modus installiert Kaspersky Endpoint Security auf dem Wechseldatenträger ein spezielles Verschlüsselungsmodul: den *portablen Dateimanager*. Der portable Dateimanager bietet eine Benutzeroberfläche für die Arbeit mit verschlüsselten Daten, wenn das Programm Kaspersky Endpoint Security nicht auf dem Computer installiert ist (s. Abb. unten). Wenn das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, können Sie einen gewöhnlichen Dateimanager (z. B. Explorer) verwenden, um mit verschlüsselten Wechseldatenträgern zu arbeiten.

Der portable Dateimanager speichert einen Schlüssel für die Verschlüsselung von Dateien auf dem Wechseldatenträger. Der Schlüssel ist mit einem Benutzerkennwort verschlüsselt. Der Benutzer legt das Kennwort fest, bevor die Dateien auf dem Wechseldatenträger verschlüsselt werden.

Der portable Dateimanager startet automatisch, wenn ein Wechseldatenträger mit einem Computer verbunden wird, auf dem das Programm Kaspersky Endpoint Security installiert ist. Wenn auf dem Computer der Autostart von Programmen deaktiviert ist, müssen Sie den portablen Dateimanager manuell starten. Führen Sie dazu die Datei pmv.exe aus, die auf dem Wechseldatenträger gespeichert ist.



Portabler Dateimanager

Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien

In der Verwaltungskonsole (MMC) die Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien auf Wechseldatenträgern aktivieren

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Wechseldatenträger verschlüsseln** aus.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** das Element **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** aus.

   Der portable Modus ist nur für die Dateiverschlüsselung (FLE) verfügbar. Die Unterstützung des portablen Modus für die vollständige Festplattenverschlüsselung (FDE) kann nicht aktiviert werden.

7. Aktivieren Sie das Kontrollkästchen **Portabler Modus**.
8. Bei Bedarf können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.
9. Speichern Sie die vorgenommenen Änderungen.
10. Nachdem Sie die Richtlinie angewendet haben, verbinden Sie den Wechseldatenträger mit dem Computer.
11. Bestätigen Sie den Vorgang zur Verschlüsselung des Wechseldatenträgers.

    Ein Fenster zum Erstellen eines Kennworts für den portablen Dateimanager wird geöffnet.
12. Legen Sie ein Kennwort fest, das den Anforderungen entspricht, und bestätigen Sie das Kennwort.
13. Klicken Sie auf **OK**.

Kaspersky Endpoint Security verschlüsselt die Dateien auf dem Wechseldatenträger. Auf dem Wechseldatenträger wird auch der portable Dateimanager für die Verwendung verschlüsselter Dateien hinzugefügt. Wenn auf dem Wechseldatenträger bereits verschlüsselte Dateien vorhanden sind, verschlüsselt Kaspersky Endpoint Security diese erneut mithilfe eines eigenen Schlüssels. Dadurch kann der Benutzer im portablen Modus auf alle Dateien des Wechseldatenträgers zugreifen.

In der „Web Console“ die Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien auf Wechseldatenträgern aktivieren

1. Wählen Sie im Hauptfenster der Web Console den Punkt **Geräte** → **Richtlinien und Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security für jene Computer, auf denen Sie die Unterstützung des portablen Modus aktivieren möchten.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Programmeinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Virtuelle Datentresore** → **Verschlüsselung von Wechseldatenträgern**.
5. Wählen Sie im Block **Verschlüsselungsverwaltung** das Element **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** aus.

   Der portable Modus ist nur für die Dateiverschlüsselung (FLE) verfügbar. Die Unterstützung des portablen Modus für die vollständige Festplattenverschlüsselung (FDE) kann nicht aktiviert werden.
6. Aktivieren Sie das Kontrollkästchen **Portabler Modus**.
7. Bei Bedarf können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.
8. Speichern Sie die vorgenommenen Änderungen.
9. Nachdem Sie die Richtlinie angewendet haben, verbinden Sie den Wechseldatenträger mit dem Computer.
10. Bestätigen Sie den Vorgang zur Verschlüsselung des Wechseldatenträgers.

    Ein Fenster zum Erstellen eines Kennworts für den portablen Dateimanager wird geöffnet.
11. Legen Sie ein Kennwort fest, das den Anforderungen entspricht, und bestätigen Sie das Kennwort.
12. Klicken Sie auf **OK**.

Kaspersky Endpoint Security verschlüsselt die Dateien auf dem Wechseldatenträger. Auf dem Wechseldatenträger wird auch der portable Dateimanager für die Verwendung verschlüsselter Dateien hinzugefügt. Wenn auf dem Wechseldatenträger bereits verschlüsselte Dateien vorhanden sind, verschlüsselt Kaspersky Endpoint Security diese erneut mithilfe eines eigenen Schlüssels. Dadurch kann der Benutzer im portablen Modus auf alle Dateien des Wechseldatenträgers zugreifen.

Zugriff auf verschlüsselte Dateien auf einem Wechseldatenträger anfordern

Nachdem Dateien auf einem Wechseldatenträger mit Unterstützung des portablen Modus verschlüsselt wurden, gibt es folgende Methoden für den Zugriff auf Dateien:

- Wenn das Programm Kaspersky Endpoint Security nicht auf dem Computer installiert ist, werden Sie vom portablen Dateimanager zur Kennworteingabe aufgefordert. Das Kennwort muss jedes Mal eingegeben werden, wenn der Computer neu gestartet oder ein Wechseldatenträger erneut verbunden wird.
- Wenn sich der Computer außerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, werden Sie vom Programm aufgefordert, das Kennwort einzugeben oder beim Administrator den Zugriff auf die Dateien anzufordern. Nachdem der Zugriff auf die Dateien des Wechseldatenträgers gewährt wurde, speichert Kaspersky Endpoint Security einen

Geheimschlüssel im Schlüsselspeicher des Computers. Dadurch ist der Dateizugriff künftig ohne Kennworteingabe oder Anfrage an den Administrator möglich.

- Wenn sich der Computer innerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, erhalten Sie ohne Kennworteingabe Zugriff auf das Gerät. Kaspersky Endpoint Security erhält einen Geheimschlüssel von dem Kaspersky Security Center Administrationsserver, mit dem der Computer verbunden ist.

Wiederherstellen des Kennworts für den portablen Modus

Wenn Sie das Kennwort für den portablen Modus vergessen haben, müssen Sie den Wechseldatenträger innerhalb des Unternehmensnetzwerks mit einem Computer verbinden, auf dem das Programm Kaspersky Endpoint Security installiert ist. Sie erhalten Zugriff auf die Dateien, da der Geheimschlüssel im Schlüsselspeicher des Computers oder auf dem Administrationsserver gespeichert ist. Entschlüsseln Sie die Dateien und verschlüsseln Sie sie dann mit einem neuen Kennwort.

Besonderheiten des portablen Modus, wenn ein Wechseldatenträger mit einem Computer aus einem anderen Netzwerk verbunden wird

Wenn sich der Computer außerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, können Sie wie folgt ohne Kennworteingabe Zugriff auf die Dateien erhalten:

- **Zugriff mit Kennwort**

  Nach der Kennworteingabe können Sie die Dateien auf dem Wechseldatenträger anzeigen, ändern und speichern (*transparenter Zugriff*). Kaspersky Endpoint Security kann für einen Wechseldatenträger das Zugriffsrecht „nur Lesen“ festlegen, wenn in den Richtlinieneinstellungen für die Verschlüsselung von Wechseldatenträgern folgende Einstellungen festgelegt sind:

  - Die Unterstützung des portablen Modus ist deaktiviert.
  - Der Modus **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** ist ausgewählt.

  In den übrigen Fällen erhalten Sie Vollzugriff auf den Wechseldatenträger (“Schreiben und Lesen“). Sie können Dateien hinzufügen und löschen.

  Sie können die Rechte für den Zugriff auf einen Wechseldatenträger auch dann ändern, wenn der Wechseldatenträger mit dem Computer verbunden ist. Wenn sich die Rechte für den Zugriff auf einen Wechseldatenträger geändert haben, blockiert Kaspersky Endpoint Security den Zugriff auf die Dateien und fragt das Kennwort erneut ab.

  Nach der Kennworteingabe können Richtlinieneinstellungen für die Verschlüsselung eines Wechseldatenträgers nicht angewendet werden. Deshalb ist es nicht möglich, die Dateien auf dem Wechseldatenträger zu entschlüsseln oder erneut zu verschlüsseln.

- **Anfrage für den Zugriff auf Dateien an den Administrator**

  Wenn Sie das Kennwort für den portablen Modus vergessen haben, fordern Sie beim Administrator den Zugriff auf die Dateien an. Für den Zugriff auf Dateien muss der Benutzer eine Zugriffsanfrage-Datei an den Administrator senden (Datei mit der Erweiterung .kesdc). Der Benutzer kann die Zugriffsanfrage-Datei beispielsweise per E-Mail senden. Der Administrator sendet eine Datei für den Zugriff auf die verschlüsselten Daten (Datei mit der Erweiterung kesdr).

  Nachdem Sie den Vorgang zur Kennwortwiederherstellung (“Anfrage-Frage“) durchlaufen haben, erhalten Sie transparenten Zugriff auf die Dateien auf dem Wechseldatenträger und Vollzugriff auf den Wechseldatenträger (Recht „Schreiben und Lesen“).

Sie können die Richtlinie für die Verschlüsselung von Wechseldatenträgern anwenden und beispielsweise Dateien entschlüsseln. Nachdem das Kennwort wiederhergestellt wurde oder wenn die Richtlinie aktualisiert wird, fordert Kaspersky Endpoint Security Sie auf, die Änderungen zu bestätigen.

In der Verwaltungskonsole (MMC) eine Zugriffsdatei für verschlüsselte Daten anfordern

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der die Wiederherstellung des Zugriffs auf verschlüsselte Daten anfordert, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.
6. Wählen Sie im folgenden Fenster die Registerkarte **Datenverschlüsselung** aus.
7. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.
8. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.

In der „Web Console“ eine Zugriffsdatei für verschlüsselte Daten anfordern

1. Wählen Sie im Hauptfenster von „Web Console“ den Punkt **Geräte → Verwaltete Geräte** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.
3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.
4. Wählen Sie den Abschnitt **Datenverschlüsselung** aus.
5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.
6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Wechseldatenträger entschlüsseln

Sie können einen Wechseldatenträger mithilfe einer Richtlinie entschlüsseln. Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Administrationsgruppe erstellt. Deshalb hängt das Ergebnis der Datenentschlüsselung auf Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Um Wechseldatenträger zu entschlüsseln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
5. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Wechseldatenträger verschlüsseln** aus.
6. Um alle verschlüsselten Dateien zu entschlüsseln, die auf Wechseldatenträgern gespeichert sind, wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion **Gesamten Wechseldatenträger entschlüsseln**.
7. Um die Daten zu entschlüsseln, die auf bestimmten Wechseldatenträgern gespeichert sind, ändern Sie die Verschlüsselungsregeln für die entsprechenden Wechseldatenträger. Gehen Sie dazu folgendermaßen vor:
   a. Wählen Sie in der Liste der Wechseldatenträger, für die Verschlüsselungsregeln vorliegen, den Eintrag des entsprechenden Wechseldatenträgers.
   b. Klicken Sie auf **Regel angeben**, um die Verschlüsselungsregel für diesen Wechseldatenträger zu ändern.
      Das Kontextmenü der Schaltfläche **Regel angeben** wird geöffnet.
   c. Wählen Sie im Kontextmenü der Schaltfläche **Regel angeben** den Punkt **Alle Dateien entschlüsseln** aus.
8. Speichern Sie die vorgenommenen Änderungen.

Wenn der Benutzer den Wechseldatenträger verbindet oder er bereits verbunden ist, entschlüsselt Kaspersky Endpoint Security den Wechseldatenträger. Das Programm warnt den Benutzer, dass die Entschlüsselung einige Zeit in Anspruch nehmen kann. Initiiert der Benutzer während der Datenentschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenentschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Entschlüsselungsvorgangs sicher zu entfernen. Die Datenentschlüsselung wird fortgesetzt, nachdem der Wechseldatenträger zum nächsten Mal mit dem Computer verbunden wird.

Wenn die Entschlüsselung des Wechseldatenträgers fehlgeschlagen ist, überprüfen Sie den Bericht **Datenverschlüsselung** auf der Benutzeroberfläche von Kaspersky Endpoint Security. Möglicherweise ist der Zugriff auf die Dateien durch ein anderes Programm gesperrt. Versuchen Sie in diesem Fall, den Wechseldatenträger vom Computer zu trennen und erneut zu verbinden.

Informationen zur Datenverschlüsselung anzeigen

Während der Verschlüsselung und Entschlüsselung von Daten erhält Kaspersky Security Center von Kaspersky Endpoint Security Informationen zum Status der Übernahme von Verschlüsselungseinstellungen auf den Client-Computern.

Für die Verschlüsselung sind folgende Statusvarianten möglich:

- *Es wurde keine Verschlüsselungsrichtlinie festgelegt*. Für den Computer wurde keine Verschlüsselungsrichtlinie für Kaspersky Security Center festgelegt.
- *Bei der Übernahme der Richtlinie*. Auf dem Computer wird die Verschlüsselung und/oder Entschlüsselung von Daten ausgeführt.
- *Fehler*. Bei der Verschlüsselung und/oder Entschlüsselung von Daten ist auf dem Computer ein Fehler aufgetreten.
- *Ein Neustart ist erforderlich*. Ein Neustart des Computers ist erforderlich, um die Verschlüsselung oder Entschlüsselung von Daten auf dem Computer zu initialisieren oder abzuschließen.
- *Entspricht der Richtlinie*. Die Datenverschlüsselung wurde auf dem Computer mit den Verschlüsselungseinstellungen ausgeführt, die der für diesen Computer übernommenen Richtlinie für Kaspersky Security Center entsprechen.
- *Vom Benutzer abgebrochen*. Der Benutzer hat den Vorgang für die Dateiverschlüsselung auf dem Wechseldatenträger nicht bestätigt.

Verschlüsselungsstatus anzeigen

Gehen Sie wie folgt vor, um die Verschlüsselungsstatus für die Daten des Computers anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

   Auf der Registerkarte **Geräte** im Arbeitsbereich werden die Eigenschaften der Computer der gewählten Administrationsgruppe angezeigt.
4. Verschieben Sie auf der Registerkarte **Geräte** im Arbeitsbereich das Bildlauffeld ganz nach rechts.
5. Falls die Spalte **Verschlüsselungsstatus** nicht angezeigt wird, gehen Sie wie folgt vor:

   a. Öffnen Sie durch Rechtsklick das Kontextmenü für den Tabellenkopf.

   b. Wählen Sie im Kontextmenü in der Dropdown-Liste **Ansicht** den Punkt **Spalten hinzufügen oder löschen** aus.

   Das Fenster **Spalten hinzufügen oder löschen** wird geöffnet.

   c. Aktivieren Sie im Fenster **Spalten hinzufügen oder löschen** das Kontrollkästchen **Verschlüsselungsstatus**.

d. Klicken Sie auf **OK**.

In der Spalte **Verschlüsselungsstatus** werden die Statusvarianten für die Datenverschlüsselung auf den Computern der ausgewählten Administrationsgruppe angezeigt. Dieser Status beruht auf Informationen über die Verschlüsselung von Dateien auf den lokalen Computerlaufwerken und über die vollständige Festplattenverschlüsselung.

Verschlüsselungsstatistik in den Informationsbereichen von Kaspersky Security Center anzeigen

Gehen Sie wie folgt vor, um die Statusmeldungen zur Dateiverschlüsselung in den Informationsbereichen von Kaspersky Security Center anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver – <Name des Computers>**.
3. Wählen Sie im Arbeitsbereich, der sich rechts von der Verwaltungskonsole befindet, die Registerkarte **Statistik**.
4. Erstellen Sie eine neue Seite mit Informationsbereichen mit einer Statistik für die Datenverschlüsselung. Gehen Sie dazu folgendermaßen vor:
   a. Klicken Sie auf der Registerkarte **Statistik** auf **Ansicht einstellen**.
      Das Fenster **Eigenschaften: Statistik**.
   b. Klicken Sie im Fenster **Eigenschaften: Statistik** auf **Hinzufügen**.
      Das Fenster **Eigenschaften: Neue Seite** wird geöffnet.
   c. Geben Sie im Abschnitt **Allgemein** des Fensters **Eigenschaften: Neue Seite** den Namen der Seite ein.
   d. Klicken Sie im Abschnitt **Informationsbereiche** auf **Hinzufügen**.
      Das Fenster **Neuer Informationsbereich** wird geöffnet.
   e. Wählen Sie im Fenster **Neuer Informationsbereich** in der Gruppe **Schutzstatus** das Element **Geräte verschlüsseln**.
   f. Klicken Sie auf **OK**.
      Das Fenster **Eigenschaften: Verschlüsselung von Geräten** wird geöffnet.
   g. Ändern Sie bei Bedarf die Einstellungen des Informationsbereichs. Verwenden Sie dazu die Abschnitte **Ansicht** und **Geräte** im Fenster **Eigenschaften: Verschlüsselung von Geräten**
   h. Klicken Sie auf **OK**.
   i. Wiederholen Sie die Punkte d – h dieser Anleitung. Wählen Sie dabei im Fenster **Neuer Informationsbereich** in der Gruppe **Schutzstatus** das Element **Wechseldatenträger verschlüsseln** aus.
      Die hinzugefügten Informationsbereiche werden in der Liste **Informationsbereiche** im Fenster **Eigenschaften: Neue Seite** angezeigt.
   j. Klicken Sie im Fenster **Eigenschaften: Neue Seite** auf **OK**.
      Der Name der Seite mit Informationsbereichen, die während der vorhergehenden Schritte erstellt wurde, erscheint in der Liste **Seiten** im Fenster **Eigenschaften: Statistik**.

k. Klicken Sie im Fenster **Eigenschaften: Statistik** auf **Schließen**.

5. Öffnen Sie auf der Registerkarte **Statistik** die Seite, die bei den vorhergehenden Schritten der Anleitung erstellt wurde.

Es werden Informationsbereiche angezeigt, in denen Sie den Verschlüsselungsstatus von Computern und Wechseldatenträgern einsehen können.

Fehler anzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten

Um Fehler anzuzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, in welcher sich der Computer befindet, für den Sie eine Fehlerliste für die Dateiverschlüsselung anzeigen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie den Computer auf der Registerkarte **Geräte** in der Liste und öffnen Sie durch Rechtsklick das Kontextmenü.
5. Wählen Sie im Kontextmenü des Computers den Punkt **Eigenschaften** aus. Wählen Sie im folgenden Fenster **Eigenschaften: <Computername>** den Abschnitt **Schutz** aus.
6. Öffnen Sie im Abschnitt **Schutz** im Fenster **Eigenschaften: <Name des Computers>** mit dem Link **Datenverschlüsselungsfehler anzeigen** das Fenster **Datenverschlüsselungsfehler**.

In diesem Fenster werden Informationen über Fehler bei der Dateiverschlüsselung auf lokalen Laufwerken angezeigt. Wenn ein Fehler korrigiert wurde, löscht Kaspersky Security Center im Fenster **Fehler bei der Dateiverschlüsselung** die Informationen dazu.

Bericht über die Datenverschlüsselung anzeigen

Gehen Sie folgendermaßen vor, um einen Bericht über die Datenverschlüsselung anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.
3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.
4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage wählen** im Abschnitt **Andere** einen der folgenden Punkte:

   - **Bericht über den Verschlüsselungsstatus der verwalteten Geräte**
   - **Bericht über den Verschlüsselungsstatus von Massenspeichergeräten**

- **Bericht über Fehler bei Dateiverschlüsselung**
- **Bericht über das Blockieren des Zugriffs auf verschlüsselte Dateien**.

Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Wählen Sie die Berichtsvorlage, die Sie bei den vorherigen Schritten der Anleitung erstellt haben.
6. Wählen Sie im Kontextmenü der Vorlage den Punkt **Bericht anzeigen** aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht

Freigabe von verschlüsselten Geräten

In folgenden Fällen kann es erforderlich sein, dass der Benutzer den Zugriff auf verschlüsselte Geräte anfordert:

- Die Festplatte wurde auf einem anderen Computer verschlüsselt.
- Auf dem Computer ist kein Chiffrierschlüssel für das Gerät vorhanden (z. B. beim ersten Zugriff auf einen verschlüsselten Wechseldatenträger auf diesem Computer) und es besteht keine Verbindung zu Kaspersky Security Center.

  Nachdem der Benutzer den Zugriffsschlüssel für ein verschlüsseltes Gerät übernommen hat, speichert Kaspersky Endpoint Security den Chiffrierschlüssel auf diesem Benutzercomputer und gibt künftig den Zugriff auf dieses Gerät frei, auch wenn keine Verbindung zu Kaspersky Security Center besteht.

Die Freigabe von verschlüsselten Geräten kann wie folgt erfolgen:

1. Der Benutzer erstellt über die Benutzeroberfläche von Kaspersky Endpoint Security eine Zugriffsanfrage-Datei mit der Erweiterung kesdc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.
2. Der Administrator erstellt in der Verwaltungskonsole von Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung kesdr und übermittelt die Datei an den Benutzer.
3. Der Benutzer wendet den Zugriffsschlüssel an.

Daten auf verschlüsselten Geräten wiederherstellen

Für die Arbeit mit verschlüsselten Geräten kann der Benutzer das Reparatur-Tool für verschlüsselte Geräte verwenden (im Folgenden „Reparatur-Tool“ genannt). Dies kann in folgenden Fällen erforderlich sein:

- Der Freigabevorgang mithilfe eines Zugriffsschlüssels ist fehlgeschlagen.
- Auf dem Computer mit dem verschlüsselten Gerät sind die Verschlüsselungskomponenten nicht installiert.

Die Daten, die erforderlich sind, um den Zugriff auf verschlüsselte Geräte mithilfe des Reparatur-Tools wiederherzustellen, befinden sich für einen bestimmten Zeitraum in unverschlüsselter Form im Arbeitsspeicher des Benutzercomputers. Um das Risiko eines unbefugten Zugriffs auf diese Daten zu reduzieren, wird empfohlen, den Wiederherstellungsvorgang nur auf vertrauenswürdigen Computern auszuführen.

Die Datenwiederherstellung auf verschlüsselten Geräten wird wie folgt ausgeführt:

1. Der Benutzer erstellt mithilfe des Reparatur-Tools eine Zugriffsanfrage-Datei mit der Erweiterung fdertc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.

2. Der Administrator erstellt in der Verwaltungskonsole für Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung fdertr und übermittelt die Datei an den Benutzer.

3. Der Benutzer wendet den Zugriffsschlüssel an.

Für die Wiederherstellung von Daten auf verschlüsselten Systemfestplatten kann der Benutzer im Reparatur-Tool auch die Anmeldedaten für den Authentifizierungsagenten angeben. Sind die Metadaten des Authentifizierungsagenten-Benutzerkontos beschädigt, so muss der Benutzer die Wiederherstellung mithilfe einer Zugriffsanfrage-Datei ausführen.

Bevor Daten auf verschlüsselten Geräten wiederhergestellt werden, sollte entweder der betreffende Computer aus der Verschlüsselungsrichtlinie für Kaspersky Security Center entnommen werden oder die Verschlüsselung in den Einstellungen der Richtlinie für Kaspersky Security Center deaktiviert werden. Dadurch wird verhindert, dass das Gerät erneut verschlüsselt wird.

Datenwiederherstellung mithilfe des Reparatur-Tools FDERT

Bei einer Fehlfunktion der Festplatte kann das Dateisystem beschädigt werden. Dann sind die Daten, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt sind, nicht verfügbar. Sie können die Daten entschlüsseln und die Daten auf einen neuen Datenträger kopieren.

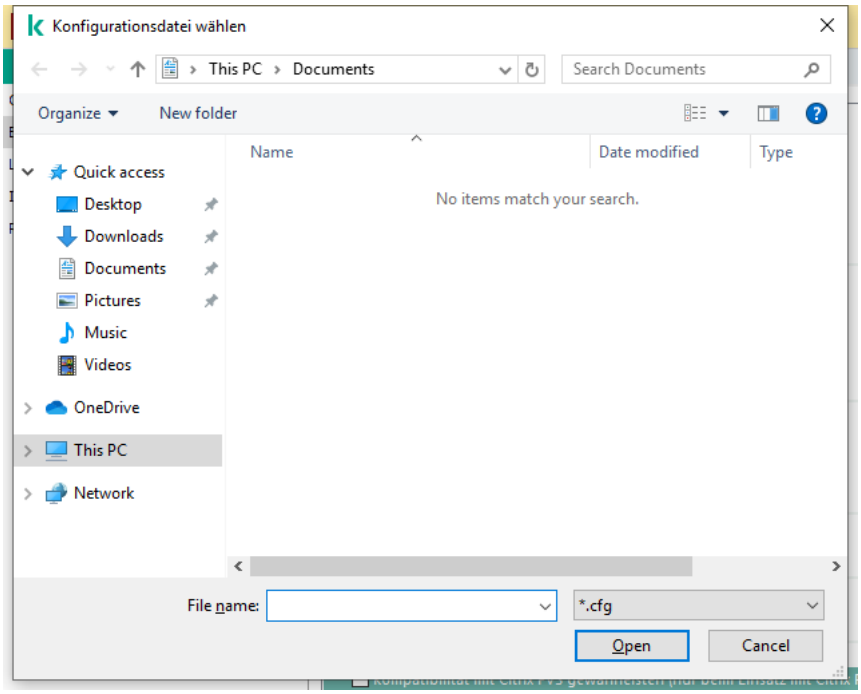
Um die Daten, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt sind, auf einem Datenträger wiederherzustellen, sind die folgenden Schritte erforderlich:

1. Erstellen eines autonomen Reparatur-Tools (s. Abb. unten).

2. Verbinden des Datenträgers mit einem Computer, auf dem die Verschlüsselungskomponenten von Kaspersky Endpoint Security nicht vorhanden sind.

3. Starten des Reparatur-Tools und der Festplatten-Analyse.

4. Zugriff auf die Daten auf dem Datenträger. Dazu müssen die Anmeldedaten des Authentifizierungsagenten eingegeben oder der Wiederherstellungsvorgang (“Anfrage-Frage“) ausgeführt werden.



FDERT-Reparatur-Tool

Erstellen eines autonomen Reparatur-Tools

Gehen Sie folgendermaßen vor, um eine ausführbare Datei des Wiederherstellungstools zu erstellen:

1. Klicken Sie im Programmhauptfenster auf **Support**.
2. Klicken Sie im folgenden Fenster auf **Verschlüsseltes Gerät wiederherstellen**.

   Das Reparatur-Tool für verschlüsselte Geräte wird gestartet.
3. Klicken Sie im Fenster des Wiederherstellungstools auf **Autonomes Reparatur-Tool erstellen**.
4. Speichern Sie das autonome Reparatur-Tool auf dem Computer.

Dadurch wird die ausführbare Datei des Wiederherstellungstools fdert.exe im angegebenen Ordner gespeichert. Kopieren Sie das Reparatur-Tool auf einen Computer, auf dem die Verschlüsselungskomponenten von Kaspersky Endpoint Security nicht vorhanden sind. Dadurch wird verhindert, dass der Datenträger erneut verschlüsselt wird.

Die Daten, die erforderlich sind, um den Zugriff auf verschlüsselte Geräte mithilfe des Reparatur-Tools wiederherzustellen, befinden sich für einen bestimmten Zeitraum in unverschlüsselter Form im Arbeitsspeicher des Benutzercomputers. Um das Risiko eines unbefugten Zugriffs auf diese Daten zu reduzieren, wird empfohlen, den Wiederherstellungsvorgang nur auf vertrauenswürdigen Computern auszuführen.

Datenwiederherstellung auf einer Festplatte

Um den Zugriff auf ein verschlüsseltes Gerät mithilfe des Reparatur-Tools wiederherzustellen, gehen Sie wie folgt vor:

1. Führen Sie die Datei mit dem Namen fdert.exe aus, die die ausführbare Datei des Wiederherstellungsprogramms ist. Diese Datei wird von Kaspersky Endpoint Security erstellt.

2. Wählen Sie im Fenster des Wiederherstellungstools in der Dropdown-Liste **Gerät auswählen** das verschlüsselte Gerät, zu dem Sie den Zugriff wiederherstellen möchten.

3. Klicken Sie auf die Schaltfläche **Diagnose**, damit das Tool feststellen kann, welche Aktion mit dem verschlüsselten Gerät ausgeführt werden soll: entsperren oder entschlüsseln.

   Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entsperren. Beim Entsperren wird das Gerät nicht entschlüsselt, es wird aber der direkte Zugriff freigegeben. Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer nicht verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entschlüsseln.

4. Um die Diagnose-Informationen zu importieren, klicken Sie auf **Diagnoseergebnisse speichern**.

   Das Tool speichert ein Archiv mit den Dateien der Diagnose-Informationen.

5. Klicken Sie auf **MBR reparieren**, wenn bei der Diagnose einer verschlüsselten Systemfestplatte Probleme gemeldet wurden, die mit dem Master Boot Record (MBR) des Geräts zusammenhängen.

   Eine Reparatur des Master Boot Records des Geräts kann den Empfang von Informationen beschleunigen, die für das Entsperren und die Entschlüsselung des Geräts benötigt werden.

6. Klicken Sie abhängig von den Ergebnissen der Diagnose auf **Entsperren** oder **Entschlüsseln**.

7. Wenn Sie die Daten mithilfe des Authentifizierungsagenten-Benutzerkontos wiederherstellen möchten, wählen Sie die Variante **Einstellungen des Benutzerkontos für den Authentifizierungsagenten verwenden** aus und geben Sie die Anmeldedaten des Authentifizierungsagenten ein.

   Diese Methode ist nur bei der Wiederherstellung von Daten auf einer Systemfestplatte möglich. Wurde die Systemfestplatte beschädigt und die Daten über das Authentifizierungsagenten-Benutzerkonto sind verloren gegangen, so muss für die Wiederherstellung von Daten auf einem verschlüsselten Gerät beim Administrator des lokalen Unternehmensnetzwerks ein Zugriffsschlüssel angefordert werden.

8. Wenn Sie den Wiederherstellungsvorgang starten möchten, gehen Sie wie folgt vor:

   a. Wählen Sie die Variante **Zugriffsschlüssel für das Gerät manuell angeben**.

   b. Klicken Sie auf **Zugriffsschlüssel anfordern** und speichern Sie die Zugriffsanfrage-Datei auf dem Computer (Datei mit der Erweiterung fdertc).

   c. Senden Sie die Zugriffsanfrage-Datei an den Administrator des lokalen Unternehmensnetzwerks.

      Schließen Sie das Fenster **Zugriffsschlüssel für das Gerät anfordern** nicht, bevor Sie einen Zugriffsschlüssel erhalten haben. Wenn dieses Fenster erneut geöffnet wird, kann der zuvor vom Administrator erstellte Zugriffsschlüssel nicht mehr verwendet werden.

   d. Speichern Sie die erhaltene Zugriffsdatei (Datei mit der Erweiterung fdertr), die der Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie übermittelt hat (s. Anleitung unten).

   e. Laden Sie die Zugriffsdatei im Fenster **Zugriffsschlüssel für das Gerät anfordern**.

9. Wenn Sie die Entschlüsselung des Gerätes ausführen, müssen weitere Entschlüsselungseinstellungen angepasst werden:

   - Geben Sie einen Bereich für die Entschlüsselung an:

     - Wenn Sie das gesamte Gerät entschlüsseln möchten, wählen Sie die Variante **Ganzes Gerät entschlüsseln**.

- Wenn Sie einen Teil der Daten auf dem Gerät entschlüsseln möchten, wählen Sie die Variante **Bestimmte Bereiche des Geräts entschlüsseln** und geben Sie die Grenzen des Entschlüsselungsbereichs an.

- Legen Sie fest, wo die entschlüsselten Daten gespeichert werden sollen:

  - Damit die Daten auf dem ursprünglichen Gerät durch die entschlüsselten Daten überschrieben werden, deaktivieren Sie das Kontrollkästchen **Entschlüsselung in eine Laufwerkabbildsdatei**.

  - Damit die entschlüsselten Daten getrennt von den verschlüsselten Quelldaten gespeichert werden, aktivieren Sie das Kontrollkästchen **Entschlüsselung in eine Laufwerkabbildsdatei** und geben Sie mithilfe der Schaltfläche **Durchsuchen** einen Pfad an, unter dem die Datei im VHD-Format gespeichert werden soll.

10. Klicken Sie auf **OK**.

Der Vorgang zum Entsperren und zur Entschlüsselung des Geräts wird gestartet.

In der Verwaltungskonsole (MMC) eine Zugriffsdatei für verschlüsselte Daten erstellen

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Geräte**.

3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät aus, für das Sie eine Zugriffsschlüsseldatei erstellen möchten, und wählen Sie den Punkt **Zugriff auf das Gerät anfordern bei Kaspersky Endpoint Security für Windows (11.6.0)** aus.

   Wenn Sie nicht sicher sind, für welchen Computer die Zugriffsanfrage-Datei erstellt wurde, wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz** aus und klicken Sie auf den Link **Chiffrierschlüssel für das Gerät anfordern bei Kaspersky Endpoint Security für Windows (11.6.0)** im Arbeitsbereich.

4. Wählen Sie im folgenden Fenster den erforderlichen Verschlüsselungsalgorithmus aus: **AES256** oder **AES56**.

   Der Algorithmus für die Datenverschlüsselung ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Strong encryption (AES256)* oder *Lite encryption (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

5. Klicken Sie auf **Durchsuchen**. Geben Sie im folgenden Fenster den Pfad der Zugriffsanfrage-Datei (mit der Erweiterung FDERTC) an, die Sie vom Benutzer erhalten haben.

6. Klicken Sie auf **Öffnen**.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.

In der „Web Console“ eine Zugriffsdatei für verschlüsselte Daten erstellen

1. Wählen Sie im Hauptfenster der „Web Control“ **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Geräte** aus.

2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, auf dem Sie die Daten wiederherstellen möchten.

3. Klicken Sie auf **Im Offline-Modus Zugriff auf das Gerät gewähren**.

   Der Assistent für die Zugriffserteilung auf das Gerät wird gestartet.

4. Folgen Sie den Anweisungen des Assistenten für die Zugriffserteilung auf das Gerät:

   a. Wählen Sie das Plug-in für **Kaspersky Endpoint Security für Windows** aus.

   b. Wählen Sie den erforderlichen Verschlüsselungsalgorithmus aus: **AES256** oder **AES56**.

      Der Algorithmus für die Datenverschlüsselung ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Strong encryption (AES256)* oder *Lite encryption (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

   c. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung fdertc).

   d. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung fdertr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Notfall-CD erstellen

Die Notfall-CD kann eingesetzt werden, wenn ein Zugriff auf die verschlüsselte Systemfestplatte nicht möglich ist und sich das Betriebssystem nicht hochfahren lässt.

Sie können mithilfe der Notfall-CD ein Abbild des Windows-Betriebssystems laden und mithilfe des im Abbild enthaltenen Wiederherstellungstools den Zugriff auf die verschlüsselte Systemfestplatte wiederherstellen.

Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Erstellen Sie eine ausführbare Datei für das Reparatur-Tool für verschlüsselte Geräte.

2. Erstellen Sie ein benutzerdefiniertes Windows PE-Abbild. Wenn Sie das benutzerdefinierte Windows PE-Abbild erstellen, fügen Sie dem Abbild die Datei des Reparatur-Tools für verschlüsselte Geräte hinzu.

3. Speichern Sie das benutzerdefinierte Windows PE-Abbild auf einem bootfähigen Medium, beispielsweise auf einer CD oder einem Wechseldatenträger.

   Eine Anleitung zum Erstellen eines benutzerdefinierten Windows PE-Abbilds finden Sie in der Microsoft-Hilfe (beispielsweise bei Microsoft TechNet).

Programm über die Befehlszeile verwalten

Sie können Kaspersky Endpoint Security über die Befehlszeile verwalten. Eine Liste der Befehle für die Programmverwaltung erhalten Sie mithilfe des Befehls `HELP`. Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, geben Sie den Befehl `HELP <Befehl>` ein.

Sonderzeichen im Befehl müssen mit Escape-Zeichen versehen werden. Escape-Zeichen &, |, (,), <, >, ^, verwenden Sie das „^“-Zeichen (z. B. um das `&`-Zeichen zu verwenden, geben Sie `^&` ein). Um das `%`-Zeichen als Escape-Zeichen zu versehen, geben Sie `%%` ein.

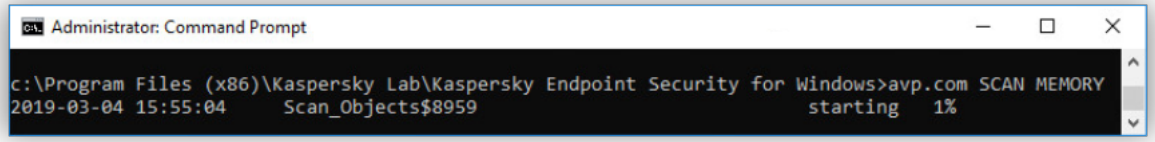
AVP-Befehle

Um Kaspersky Endpoint Security über die Befehlszeile zu verwalten, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

```
avp.com <Befehl> [Parameter]
```

Dadurch führt Kaspersky Endpoint Security den Befehl aus (siehe Abbildung unten).



Programm über die Befehlszeile verwalten

SCAN. Untersuchung auf Viren

Aufgabe zur Virenuntersuchung starten.

Befehlssyntax

```
SCAN [<Untersuchungsbereich>] [<Aktion beim Fund einer Bedrohung>] [<Dateitypen>]
[<Untersuchungsausnahmen>] [/R[A]:<Berichtsdatei>] [<Untersuchungstechnologien>] [/C:
<Datei mit Einstellungen für die Untersuchung auf Viren>]
```

Untersuchungsbereich	
`<Zu untersuchende`	Liste mit Dateien und Ordner, durch Leerzeichen getrennt. Lange Pfade müssen in

`Dateien>`	Anführungszeichen gesetzt werden. Kurze Pfade (Formate MS-DOS) müssen nicht in Anführungszeichen stehen. Beispielsweise: • `“C:\Program Files (x86)\Example Folder”` – langer Pfad. • `C:\PROGRA~2\EXAMPL~1` – kurzer Pfad.
`/ALL`	Aufgabe *Vollständige Untersuchung* starten. Kaspersky Endpoint Security untersucht folgende Objekte: • Arbeitsspeicher des Kerns • Objekte, die beim Hochfahren des Betriebssystems geladen werden • Bootsektoren • Backup des Betriebssystems • alle Festplatten und Wechseldatenträger
`/MEMORY`	Untersuchung des Kernel-Speichers
`/STARTUP`	Untersuchung der Objekte, die beim Hochfahren des Betriebssystems geladen werden
`/MAIL`	Untersuchung des Outlook-E-Mail-Postfachs
`/REMDRIVES`	Wechseldatenträger untersuchen.
`/FIXDRIVES`	Festplatten untersuchen.
`/NETDRIVES`	Netzlaufwerke untersuchen.
`/QUARANTINE`	Dateien im Backup von Kaspersky Endpoint Security untersuchen.
`/@:<Liste der Dateien.lst>`	Untersuchung der Dateien und Ordner, die in der Liste angegeben sind. Jede Datei in der Liste muss in einer separaten Zeile stehen. Lange Pfade müssen in Anführungszeichen gesetzt werden. Kurze Pfade (Formate MS-DOS) müssen nicht in Anführungszeichen stehen. Beispielsweise: • `“C:\Program Files (x86)\Example Folder”` – langer Pfad. • `C:\PROGRA~2\EXAMPL~1` – kurzer Pfad.

Aktion beim Fund einer Bedrohung	
`/i0`	Informieren. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
`/i1`	Desinfizieren; blockieren, wenn Desinfektion fehlschlägt. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.
`/i2`	Desinfizieren; löschen, wenn Desinfektion fehlschlägt. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren.

	Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. Diese Aktion ist standardmäßig ausgewählt.
`/i3`	Gefundene infizierte Dateien desinfizieren. Falls eine Desinfektion nicht möglich ist, infizierte Dateien löschen. Auch zusammengesetzte Dateien (z. B. Archive) löschen, wenn die infizierte Datei nicht desinfiziert oder gelöscht werden kann.
`/i4`	Infizierte Dateien löschen. Auch zusammengesetzte Dateien (z. B. Archive) löschen, wenn die infizierte Datei nicht gelöscht werden kann.
`/i8`	Den Benutzer sofort nach dem Fund einer Bedrohung nach einer Aktion fragen.
`/i9`	Den Benutzer nach der Untersuchung nach einer Aktion fragen.

Dateitypen	
`/fe`	Dateien nach Erweiterung untersuchen. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.
`/fi`	Dateien nach Format untersuchen. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht.
`/fa`	Alle Dateien. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). Diese Option ist standardmäßig voreingestellt.

Untersuchungsausnahmen	
`-e:a`	Archive der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE von der Untersuchung ausschließen.
`-e:b`	E-Mail-Datenbanken, die ein- und ausgehende E-Mail-Nachrichten enthalten, von der Untersuchung ausschließen.
`-e:<Dateimaske>`	Dateien nach einer Maske von der Untersuchung ausschließen. Beispielsweise: • Die Maske `*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe. • Die Maske `Beispiel*` umfasst alle Pfade von Dateien mit dem Namen BEISPIEL.
`-e:<Sekunden>`	Dateien, deren Untersuchung die in Sekunden vorgegebene Dauer überschreitet, von der Untersuchung ausschließen.
`-es:<Megabyte>`	Dateien, deren Größe den in Megabyte vorgegebenen Wert überschreitet, von der Untersuchung ausschließen.

Modus zur Speicherung von Ereignissen in der Berichtsdatei	
`/R:<Berichtsdatei>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<Berichtsdatei>`	Alle Ereignisse in der Berichtsdatei speichern.

Untersuchungstechnologien	
`/iChecker=on|off`	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
`/iSwift=on|off`	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

Erweiterte Einstellungen	
`/C:<Datei mit Einstellungen für die Virenuntersuchung>`	Datei mit Einstellungen für die Aufgabe zur Virenuntersuchung. Die Datei muss manuell erstellt und im TXT-Format gespeichert werden. Die Datei kann den folgenden Inhalt haben: `[<Untersuchungsbereich>] [<Aktion beim Fund einer Bedrohung>] [<Dateitypen>] [<Untersuchungsausnahmen>] [/R[A]:<Berichtsdatei>] [<Untersuchungstechnologien>]`.

Beispiel:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL „C:\Documents and Settings\All Users\My Documents“ „C:\Program Files”
```

UPDATE. Update der Datenbanken und Programm-Module

Aufgabe *Update* starten.

Befehlssyntax

```
UPDATE [local] ["<Update-Quelle>"] [/R[A]:<Berichtsdatei>] [/C:<Datei mit Update-Einstellungen>]
```

Einstellungen für Update-Aufgaben	
`local`	Start der *Update-Aufgabe*, die nach der Installation des Programms automatisch erstellt wurde. Sie können die Einstellungen der *Update*-Aufgabe in der lokalen Programmoberfläche oder in der Konsole von Kaspersky Security Center ändern. Wenn diese Einstellung nicht konfiguriert ist, startet Kaspersky Endpoint Security die *Update*-Aufgabe mit den Standardeinstellungen oder mit den im Befehl angegebenen Einstellungen. Sie können die Einstellungen der Update-Aufgabe wie folgt konfigurieren:

	• `UPDATE` startet die *Update*-Aufgabe mit den Standardeinstellungen: Als Update-Quelle dienen die Kaspersky-Update-Server, das Benutzerkonto ist System, und weitere Standardeinstellungen. • `UPDATE local` startet die *Update*-Aufgabe, die nach der Installation automatisch erstellt wurde (vordefinierte Aufgabe). • `UPDATE <Update-Einstellungen>` startet die *Update*-Aufgabe mit manuell festgelegten Einstellungen (siehe unten).

Update-Quelle	
`"<Update-Quelle>"`	Adresse eines HTTP- oder FTP-Servers oder eines gemeinsamen Ordners mit dem Update-Paket. Sie können nur eine Update-Quelle angeben. Wenn die Update-Quelle nicht angegeben wird, verwendet Kaspersky Endpoint Security die Standardquelle: Kaspersky Update-Server.

Modus zur Speicherung von Ereignissen in der Berichtsdatei	
`/R:<Berichtsdatei>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<Berichtsdatei>`	Alle Ereignisse in der Berichtsdatei speichern.

Erweiterte Einstellungen	
`/C:<Datei mit Update-Einstellungen>`	Datei mit Einstellungen für die Aufgabe *Update*. Die Datei muss manuell erstellt und im TXT-Format gespeichert werden. Die Datei kann den folgenden Inhalt haben: `["<Update-Quelle>"] [/R[A]:<Berichtsdatei>]`.

Beispiel:

```
avp.com UPDATE local

avp.com UPDATE „ftp://my_server/kav updates“ /RA:avbases_upd.txt
```

ROLLBACK. Letztes Update rückgängig machen

Letztes Update der Antiviren-Datenbanken rückgängig machen. Dadurch besteht die Möglichkeit, bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückzukehren. Dies ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, welche dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert.

Befehlssyntax

```
ROLLBACK [/R[A]:<Berichtsdatei>]
```

Modus zur Speicherung von Ereignissen in der Berichtsdatei	

`/R:<Berichtsdatei>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<Berichtsdatei>`	Alle Ereignisse in der Berichtsdatei speichern.

Beispiel:
`avp.com ROLLBACK /RA:rollback.txt`

TRACES. Protokollierung von Ereignissen

Protokollierung aktivieren/deaktivieren. Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird. Ablaufverfolgungsdateien werden gespeichert im Ordner %ProgramData%\Kaspersky Lab\KES\Traces. Eine Ausnahme bilden die Ablaufverfolgungsdateien des Authentifizierungsagenten. Die Protokollierung ist standardmäßig deaktiviert.

Befehlssyntax

```
TRACES on|off [<Ablaufverfolgungsstufe>] [<erweiterte Einstellungen>]
```

Ablaufverfolgungsstufe	
`<Ablaufverfolgungsstufe>`	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • `100` (kritisch). Nur Meldungen über fatale Fehler. • `200` (hoch). Meldungen über alle Fehler, einschließlich fatale. • `300` (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • `400` (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • `500` (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über die Nutzung des Programms im normalen Modus (Standardwert). • `600` (niedrig). Alle Meldungen.

Erweiterte Einstellungen	
`all`	Befehl mit den Parametern `dbg`, `file` und `mem` ausführen.
`dbg`	Funktion OutputDebugString verwenden und Protokolldatei speichern. Die Funktion OutputDebugString sendet eine Zeichenfolge an den Programm-Debugger zur Anzeige auf dem Bildschirm. Details finden Sie auf der *MSDN-Website*.
`file`	Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).
`rot`	Protokollierungsergebnisse in einer beschränkten Anzahl von Dateien mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird.
`mem`	Protokollierungsergebnisse in Dump-Dateien speichern.

Beispiele:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Profil starten

Ausführung des Profils starten (z. B. Update der Datenbanken starten oder Schutzkomponente aktivieren).

Befehlssyntax

```
START <Profil> [/R[A]:<Berichtsdatei>]
```

Profil	
`<Profil>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP START`.

Modus zur Speicherung von Ereignissen in der Berichtsdatei	
`/R:<Berichtsdatei>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<Berichtsdatei>`	Alle Ereignisse in der Berichtsdatei speichern.

Beispiel:
`avp.com START Scan_Objects`

STOP. Profil beenden

Ausführbares Profil beenden (z. B. Untersuchung von Wechseldatenträgern beenden oder Schutzkomponente deaktivieren).

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigungen **Schutzkomponenten deaktivieren** und **Kontrollkomponenten deaktivieren** haben.

Befehlssyntax

```
STOP <Profil> /login=<Benutzername> /password=<Kennwort>
```

Profil	
`<Profil>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STOP`.

Autorisierung	
`/login=<Benutzername>` `/password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

STATUS. Status des Profils

Informationen über den Status von Programmprofilen anzeigen (z. B. `running` oder `completed`). Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STATUS`.

Außerdem zeigt Kaspersky Endpoint Security Informationen über den Status von Dienstprofilen an. Informationen über den Status von Dienstprofilen können erforderlich sein, wenn Sie sich an den Technischen Support von Kaspersky wenden.

Befehlssyntax

```
STATUS [<Profil>]
```

STATISTICS. Ausführungsstatistik für das Profil

Statistische Informationen über ein Programmprofil anzeigen (z. B. Untersuchungsdauer oder Anzahl der gefundenen Bedrohungen). Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STATISTICS`.

Befehlssyntax

```
STATISTICS <Profil>
```

RESTORE. Dateien wiederherstellen

Datei aus dem Backup in ihrem ursprünglichen Speicherort wiederherstellen. Wenn am angegeben Pfad bereits eine Datei mit diesem Namen vorhanden ist, erhält der Dateiname das Suffix „-copy“. Die wiederherzustellende Datei wird mit ihrem ursprünglichen Namen kopiert.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Wiederherstellung aus dem Backup** besitzen.

Das *Backup* ist ein Speicher für Backup-Kopien von Dateien, die bei der Desinfektion verändert oder gelöscht wurden. Eine *Backup-Kopie* ist die Kopie einer Datei, die vor der Desinfektion oder dem Löschen dieser Datei angelegt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Backup-Kopien von Dateien werden im Ordner `C:\ProgramData\Kaspersky Lab\KES\QB` gespeichert.

Vollständige Zugriffsrechte auf diesen Ordner besitzen die Benutzer der Gruppe „Administratoren“. Beschränkte Zugriffsrechte für diesen Ordner besitzt der Benutzer, unter dessen Benutzerkonto die Installation von Kaspersky Endpoint Security ausgeführt wurde.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Befehlssyntax

```
RESTORE [/REPLACE] <Dateiname> /login=<Benutzername> /password=<Kennwort>
```

Erweiterte Einstellungen	
`/REPLACE`	Vorhandene Datei überschreiben.
`<Dateiname>`	Name der wiederherzustellenden Datei.

Autorisierung	
`/login=<Benutzername>` `/password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Programmeinstellungen exportieren

Einstellungen für Kaspersky Endpoint Security in eine Datei exportieren. Die Datei wird im Ordner C:\Windows\SysWOW64 abgelegt.

Befehlssyntax

```
EXPORT <Profil> <Dateiname>
```

Profil	
`<Profil>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP EXPORT`.

Datei für den Export	
`<Dateiname>`	Name der Datei, in welche die Profileinstellungen exportiert werden sollen. Sie können die Profileinstellungen in eine Konfigurationsdatei im DAT- oder CFG-Format, in eine Textdatei

	im TXT-Format oder in ein Dokument im XML-Format exportieren.

Beispiele:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Programmeinstellungen importieren

Einstellungen für Kaspersky Endpoint Security aus einer Datei importieren, die mithilfe des Befehls `EXPORT` erstellt wurde.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Programmeinstellungen anpassen** besitzen.

Befehlssyntax

```
IMPORT <Dateiname> /login=<Benutzername> /password=<Kennwort>
```

Datei für den Import	
`<Dateiname>`	Name der Datei, aus welcher die Programmeinstellungen importiert werden sollen. Sie können die Einstellungen für Kaspersky Endpoint Security aus einer Konfigurationsdatei im DAT- oder CFG-Format, einer Textdatei im TXT-Format oder einem Dokument im XML-Format importieren.

Autorisierung	
`/login=<Benutzername> /password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel:
`avp.com IMPORT config.dat /login=KLAdmin /password=!Password1`

ADDKEY. Schlüsseldatei übernehmen

Schlüsseldatei für die Aktivierung von Kaspersky Endpoint Security übernehmen. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.

Befehlssyntax

```
ADDKEY <Dateiname> [/login=<Benutzername> /password=<Kennwort>]
```


Schlüsseldatei	
`<Dateiname>`	Name der Schlüsseldatei.

Autorisierung	
`/login=<Benutzername> /password=<Kennwort>`	Daten des Benutzerkontos. Die Daten des Benutzerkontos müssen nur eingegeben werden, wenn der Kennwortschutz aktiviert ist.

Beispiel:
```
avp.com ADDKEY file.key
```

LICENSE. Lizenzverwaltung

Vorgänge mit den Lizenzschlüsseln des Programms Kaspersky Endpoint Security ausführen.

Damit der Befehl zum Löschen eines Lizenzschlüssels ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Schlüssel löschen** besitzen.

Befehlssyntax

```
LICENSE <Vorgang> [/login=<Benutzername> /password=<Kennwort>]
```

Vorgang	
`/ADD <Dateiname>`	Schlüsseldatei für die Aktivierung von Kaspersky Endpoint Security übernehmen. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.
`/ADD <Aktivierungscode>`	Kaspersky Endpoint Security mithilfe eines Aktivierungscodes aktivieren. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.
`/REFRESH <Dateiname>`	Gültigkeitsdauer der Lizenz mithilfe einer Schlüsseldatei verlängern. Als Ergebnis wird ein Reserveschlüssel hinzugefügt. Er wird nach Ablauf der Lizenz aktiv. Ein aktiver Schlüssel kann mit diesem Befehl nicht hinzugefügt werden.
`/REFRESH <Aktivierungscode>`	Gültigkeitsdauer der Lizenz mithilfe eines Aktivierungscodes verlängern. Als Ergebnis wird ein Reserveschlüssel hinzugefügt. Er wird nach Ablauf der Lizenz aktiv. Ein aktiver Schlüssel kann mit diesem Befehl nicht hinzugefügt werden.
`/DEL /login= <Benutzername> /password= <Kennwort>`	Lizenzschlüssel löschen. Der Reserveschlüssel wird ebenfalls gelöscht.

Autorisierung	
`/login=<Benutzername> /password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel:

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Lizenz kaufen

Zur Kaspersky-Website wechseln, um eine Lizenz zu kaufen oder die Lizenz zu verlängern.

PBATESTRESET. Untersuchungsergebnisse vor der Datenträgerverschlüsselung zurücksetzen

Zurücksetzen der Überprüfungsergebnisse für die Unterstützung der vollständigen Festplattenverschlüsselung (FDE) mithilfe der Kaspersky-Festplattenverschlüsselung und der BitLocker-Laufwerkverschlüsselung.

Vor dem Start der vollständigen Festplattenverschlüsselung führt das Programm eine Reihe von Untersuchungen aus. Dabei wird überprüft, ob der Computer verschlüsselt werden kann. Wenn eine vollständige Festplattenverschlüsselung nicht möglich ist, speichert Kaspersky Endpoint Security Informationen über die Inkompatibilität. Beim nächsten Verschlüsselungsversuch führt das Programm keine Überprüfung aus und warnt davor, dass eine Verschlüsselung nicht möglich ist. Wenn die Hardware-Konfiguration des Computers verändert wurde und anschließend die Systemfestplatte auf Kompatibilität mit der Technologie Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung überprüft werden soll, müssen zuerst die Inkompatibilitätsinformationen zurückgesetzt werden, die das Programm bei der vorherigen Überprüfung ermittelt hat.

EXIT. Programm beenden

Kaspersky Endpoint Security beenden. Das Programm wird aus dem Arbeitsspeicher des Computers entladen.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Programm beenden** besitzen.

Befehlssyntax

```
EXIT /login=<Benutzername> /password=<Kennwort>
```

EXITPOLICY. Richtlinie deaktivieren.

Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss (🔒) haben.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Richtlinie für Kaspersky Security Center deaktivieren** besitzen.

Befehlssyntax

```
EXITPOLICY /login=<Benutzername> /password=<Kennwort>
```

STARTPOLICY. Richtlinie aktivieren

Richtlinie für Kaspersky Security Center auf dem Computer aktivieren. Die Programmeinstellungen werden gemäß der Richtlinie angepasst.

DISABLE. Schutz deaktivieren

Deaktivierung des „Schutzes vor bedrohlichen Dateien“ auf einem Computer mit einer abgelaufenen Lizenz für Kaspersky Endpoint Security. Dieser Befehl kann nicht ausgeführt werden auf einem Computer, auf dem das Programm nicht aktiviert ist oder auf dem eine aktuelle Lizenz vorliegt.

SPYWARE. Spyware erkennen

Erkennung von Spyware aktivieren/deaktivieren. Die Spyware-Erkennung ist standardmäßig aktiviert.

Befehlssyntax

```
SPYWARE on|off
```

MDRLICENSE. MDR-Aktivierung

Führen Sie Vorgänge mit der BLOB-Konfigurationsdatei aus, um „Managed Detection and Response“ zu aktivieren. Die BLOB-Datei enthält die Client-ID und Informationen zur Lizenz für Kaspersky Managed Detection and Response. Die BLOB-Datei befindet sich im ZIP-Archiv der MDR-Konfigurationsdatei. Sie können das ZIP-Archiv in der Konsole von Kaspersky Managed Detection and Response abrufen. Ausführliche Informationen zur BLOB-Datei *finden Sie in der Hilfe zu Kaspersky Managed Detection and Response*.

Für die Ausführung von Vorgängen mit einer BLOB-Datei sind Administratorrechte erforderlich. Auch die Einstellungen von „Managed Detection and Response“ in der Richtlinie müssen zur Bearbeitung verfügbar sein ( ).

Befehlssyntax

```
MDRLICENSE <Vorgang> [/login=<Benutzername> /password=<Kennwort>]
```

Vorgang	
`/ADD <Dateiname>`	Wenden Sie die BLOB-Konfigurationsdatei an, um die Integration in Kaspersky Managed Detection and Response zu ermöglichen (Dateiformat p7). Sie können nur eine einzige BLOB-Datei anwenden. Wenn dem Computer bereits eine BLOB-Datei hinzugefügt wurde, wird die Datei ersetzt.
`/DEL`	Löschen Sie die BLOB-Konfigurationsdatei.

Autorisierung	
`/login=<Benutzername> /password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel:

- `avp.com MDRLICENSE /ADD file.key`
- `avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1`

KSN. Übergang von Global/Private KSN

Auswahl einer Lösung von Kaspersky Security Network zur Ermittlung der Reputation von Dateien und Websites. Kaspersky Endpoint Security unterstützt die folgenden KSN-Infrastruktur-Lösungen:

- Die Lösung *Global KSN* wird von den meisten Kaspersky-Programmen verwendet. Die KSN-Teilnehmer erhalten von Kaspersky Security Network Informationen und senden an Kaspersky bestimmte Daten über Objekte, die auf dem Benutzercomputer gefunden wurden. Auf diese Weise können die Daten zusätzlich durch die Kaspersky-Analytiker untersucht werden, und die Reputations- und Statistik-Datenbanken von Kaspersky Security Network werden ergänzt.
- Die Lösung *Private KSN* ermöglicht Benutzern den Zugriff auf die Reputations-Datenbanken und auf andere statistische Daten, ohne dabei Daten von den Benutzercomputern an KSN zu senden. Auf diesen Computern müssen das Programm Kaspersky Endpoint Security oder andere Kaspersky-Programme installiert sein. Private KSN wurde für Unternehmenskunden entwickelt, die z. B. aus folgenden Gründen keine Möglichkeit zur Teilnahme an Kaspersky Security Network haben:
  - Lokale Arbeitsplätze haben keinen Internetzugriff.
  - Es ist gesetzlich verboten oder durch die Unternehmenssicherheit beschränkt, beliebige Daten in andere Länder oder aus dem lokalen Unternehmensnetzwerk heraus zu senden.

Befehlssyntax

```
KSN /global | /private <Dateiname>
```

Konfigurationsdatei für Private KSN	
`<Dateiname>`	Name der Konfigurationsdatei mit den Einstellungen des KSN-Proxyservers. Diese Datei hat die Erweiterung pkcs7 oder pem.

Beispiel:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

KESCLI-Befehle

Mit KESCLI-Befehlen können Sie unter Verwendung der OPSWAT-Komponente Informationen über den Status des Computerschutzes erhalten und Standardaufgaben wie Virenuntersuchungen und Datenbanken-Updates ausführen.

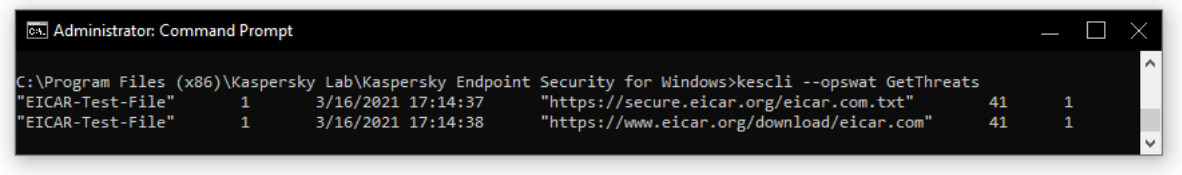
Eine Liste der KESCLI-Befehle erhalten Sie mit dem Befehl `--help` oder mit dem Kurzbefehl `-h`.

Um Kaspersky Endpoint Security über die Befehlszeile zu verwalten, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

   ```
   kescli <Befehl> [Parameter]
   ```

   Dadurch führt Kaspersky Endpoint Security den Befehl aus (siehe Abbildung unten).



Programm über die Befehlszeile verwalten

Scan. Untersuchung auf Viren

Aufgabe zur Virenuntersuchung starten.

Befehlssyntax

```
--opswat Scan <Untersuchungsbereich> <Aktion bei der Bedrohungserkennung>
```

Den Abschluss-Status der Aufgabe *Vollständige Untersuchung* können Sie mithilfe des Befehls `GetScanState` überprüfen. Außerdem können Sie mit dem Befehl `GetLastScanTime` den Zeitpunkt (Datum und Uhrzeit) anzeigen, zu dem die Untersuchung zuletzt abgeschlossen wurde.

Untersuchungsbereich	
`<Zu untersuchende`	`;` Liste mit Dateien und Ordner, durch Leerzeichen getrennt. Zum Beispiel:

Dateien>	`C:\Program Files (x86)\Beispielordner`.

Aktion beim Fund einer Bedrohung	
`0`	Informieren. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
`1`	Desinfizieren; löschen, wenn Desinfektion fehlschlägt. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. Diese Aktion ist standardmäßig ausgewählt.

Beispiel:
```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. Abschluss-Status der Untersuchung

Abrufen von Informationen über den Abschluss-Status der Aufgabe *Vollständige Untersuchung*:

- `1` – die Untersuchung läuft.
- `0` – die Untersuchung läuft nicht.

Befehlssyntax
```
--opswat GetScanState
```

Beispiel:
```
kescli --opswat GetScanState
```

GetLastScanTime. Abschlusszeit der Untersuchung festlegen

Abrufen von Informationen über den Zeitpunkt (Datum und Uhrzeit), zu dem die Aufgabe *Vollständige Untersuchung* zuletzt abgeschlossen wurde.

Befehlssyntax
```
--opswat GetLastScanTime
```

Beispiel:
```
kescli --opswat GetLastScanTime
```

GetThreats. Daten über erkannte Bedrohungen abrufen

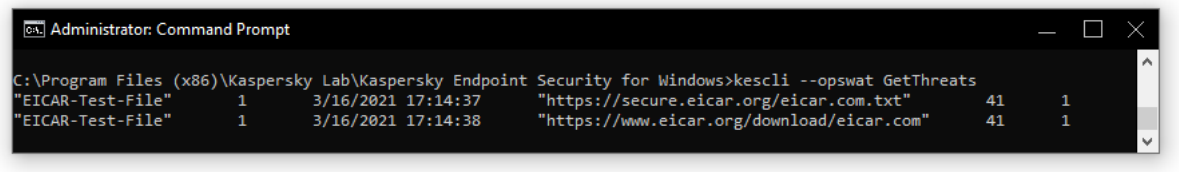
Abrufen von einer Liste der erkannten Bedrohungen (*Bedrohungsbericht*). Dieser Bericht enthält Informationen über die Bedrohungen und die Virenaktivität während der letzten 30 Tage bevor der Bericht erstellt wurde.

Befehlssyntax

```
--opswat GetThreats
```

Wenn dieser Befehl ausgeführt wird, sendet Kaspersky Endpoint Security eine Antwort mit dem folgenden Format:

`<Name des erkannten Objekts>` `<Typ des Objekts>` `<Datum und Uhrzeit der Erkennung>` `<Dateipfad>` `<Aktion bei der Bedrohungserkennung>` `<Gefahrenstufe der Bedrohung>`



Programm über die Befehlszeile verwalten

Typ des Objekts	
`0`	Unbekannt (`Unknown`).
`1`	Viren (`Virware`).
`2`	Trojaner (`Trojware`).
`3`	Schadsoftware (`Malware`).
`4`	Adware (`Adware`).
`5`	Dialer-Programme (`Pornware`).
`6`	Anwendungen, mit denen Cyberkriminelle den Computer oder die Benutzerdaten beschädigen können (`Riskware`).
`7`	Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kann (`Packed`).
`20`	Unbekannte Objekte (`Xfiles`).
`21`	Bekannte Anwendungen (`Software`).
`22`	Verdeckte Dateien (`Hidden`).
`23`	Anwendung, die Aufmerksamkeit erfordert (`Pupware`).
`24`	Anomales Verhalten (`Anomaly`).
`30`	Nicht ermittelt (`Undetect`).
`40`	Werbebanner (`Banner`).
`50`	Netzwerkangriff (`Attack`).
`51`	Registrierungszugriff (`Registry`).

52	Verdächtige Aktivität (`Suspicion`).
60	Schwachstellen (`Vulnerability`).
70	`Phishing`.
80	Unerwünschter E-Mail-Anhang (`Attachment`).
90	Schadsoftware, die von Kaspersky Security Network erkannt wurde (`Urgent`).
100	Unbekannter Link (`Suspic URL`).
110	Andere Schadsoftware (`Behavioral`).

Aktion beim Fund einer Bedrohung	
0	Unbekannt (`unknown`).
1	Bedrohung wurde neutralisiert (`ok`).
2	Objekt war infiziert und wurde nicht desinfiziert (`infected`).
5	Objekt befindet sich in einem Archiv und wurde nicht desinfiziert (`archive`).
9	Objekt wurde desinfiziert (`disinfected`).
10	Objekt wurde nicht desinfiziert (`not disinfected`).
11	Objekt wurde gelöscht (`deleted`).
13	Eine Backup-Kopie des Objekts wurde erstellt (`backupped`).
15	Objekt wurde ins Backup verschoben (`quarantined`).
23	Objekt wurde beim Neustart des Computers gelöscht (`delete on reboot`).
25	Objekt wurde beim Neustart des Computers desinfiziert (`disinfect on reboot`).
29	Objekt wurde vom Benutzer ins Backup verschoben (`added by user`).
30	Objekt wurde zu den Ausnahmen hinzugefügt (`added to exclude`).
31	Objekt wurde beim Neustart des Computers ins Backup verschoben (`quarantine on reboot`).
36	Fehlalarm (`false alarm`).
38	Prozess wurde beendet (`terminated`).
40	Objekt wurde nicht erkannt (`not found`).
41	Bedrohung kann nicht neutralisiert werden (`untreatable`).
42	Objekt wurde wiederhergestellt (`rolled back`).
43	Objekt wurde aufgrund einer Bedrohungsaktivität erstellt (`produced by threat`).
44	Objekt wurde beim Neustart des Computers wiederhergestellt (`roll back on reboot`).
0xffffffff	Objekt wurde nicht bearbeitet (`discarded`).

Gefahrenstufe der Bedrohung	

`0`	Unbekannt
`1`	Hoch
`2`	Mittlere Untersuchung
`4`	Niedrig
`8`	Info (niedriger als *Niedrig*)

UpdateDefinitions. Update der Datenbanken und Programm-Module

Aufgabe *Update* starten. Kaspersky Endpoint Security verwendet die Standardquelle: Kaspersky-Update-Server.

Befehlssyntax

```
--opswat UpdateDefinitions
```

Den Zeitpunkt (Datum und Uhrzeit), zu dem die Aufgabe *Update* zuletzt abgeschlossen wurde, können Sie mit dem Befehl `GetDefinitionsetState` anzeigen.

Beispiel:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Abschlusszeit des Updates ermitteln

Abrufen von Informationen über den Zeitpunkt (Datum und Uhrzeit), zu dem die Aufgabe *Update* zuletzt abgeschlossen wurde.

Befehlssyntax

```
--opswat GetDefinitionState
```

Beispiel:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Schutz aktivieren

Aktivieren der Schutzkomponenten von Kaspersky Endpoint Security auf dem Computer: Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Schutz vor Netzwerkbedrohungen, Programm-Überwachung.

Befehlssyntax

```
--opswat EnableRTP
```

Den Betriebsstatus des „Schutzes vor bedrohlichen Dateien“ können Sie mit dem Befehl `GetRealTimeProtectionState` überprüfen.

Beispiel:
`kescli --opswat EnableRTP`

GetRealTimeProtectionState. Status des „Schutzes vor bedrohlichen Dateien“

Abrufen von Informationen über den Betriebsstatus der Komponente „Schutz vor bedrohlichen Dateien“:

- `1` – die Komponente ist aktiviert.
- `0` – die Komponente ist deaktiviert.

Befehlssyntax

```
--opswat GetRealTimeProtectionState
```

Beispiel:
`kescli --opswat GetRealTimeProtectionState`

Version. Anwendungsversion ermitteln

Version von Kaspersky Endpoint Security für Windows ermitteln.

Befehlssyntax

```
--Version
```

Sie können auch den Kurzbefehl `-v` verwenden.

Beispiel:
`kescli -v`

Fehlercodes

Wenn das Programm über die Befehlszeile verwaltet wird, können Fehler auftreten. Wenn ein Fehler auftritt, zeigt Kaspersky Endpoint Security eine Fehlermeldung an, z. B. `Error: Cannot start task 'EntAppControl'`. Außerdem kann Kaspersky Endpoint Security zusätzliche Angaben in Form eines Codes anzeigen, z. B. `error=8947906D` (s. folgende Tabelle).

Fehlercodes

Fehlercode	Beschreibung
`09479001`	Der Lizenzschlüssel für Kaspersky Endpoint Security wird bereits auf diesem Computer

	verwendet.
0947901D	Die Lizenz ist abgelaufen. Das Datenbanken-Update ist nicht verfügbar.
89479002	Schlüssel nicht gefunden.
89479003	Die digitale Signatur ist beschädigt oder fehlt.
89479004	Es sind beschädigte Daten vorhanden.
89479005	Die Schlüsseldatei ist beschädigt.
89479006	Die Lizenz oder der Lizenzschlüssel ist abgelaufen.
89479007	Es wurde keine Schlüsseldatei angegeben.
89479008	Diese Schlüsseldatei kann nicht verwendet werden.
89479009	Das Speichern von Daten ist fehlgeschlagen.
8947900A	Das Lesen von Daten ist fehlgeschlagen.
8947900B	Eingabe-/Ausgabefehler.
8947900C	Die Datenbanken wurden nicht gefunden.
8947900E	Die Lizenzierungsbibliothek wurde nicht geladen.
8947900F	Die Datenbanken sind beschädigt oder wurden manuell aktualisiert.
89479010	Die Datenbanken sind beschädigt.
89479011	Eine ungültige Schlüsseldatei kann nicht verwendet werden, um einen Reserveschlüssel hinzuzufügen.
89479012	Systemfehler.
89479013	Denyliste der Schlüssel beschädigt.
89479014	Die Dateisignatur stimmt nicht mit der digitalen Kaspersky-Signatur überein.
89479015	Ein Schlüssel für eine nicht-kommerzielle Lizenz kann nicht als Schlüssel für eine kommerzielle Lizenz verwendet werden.
89479016	Eine Lizenz für Beta-Tests ist erforderlich, um eine Beta-Version des Programms zu verwenden.
89479017	Die Schlüsseldatei passt nicht zu diesem Programm.
89479018	Der Schlüssel wurde von Kaspersky gesperrt.
89479019	Das Programm wurde bereits mit einer Testlizenz verwendet. Es ist nicht möglich, erneut einen Schlüssel für eine Testlizenz hinzuzufügen.
8947901A	Die Schlüsseldatei ist beschädigt.
8947901B	Die digitale Signatur wurde nicht gefunden, ist beschädigt oder weicht von der Kaspersky-Signatur ab.
8947901C	Ein Schlüssel kann nicht hinzugefügt werden, wenn die entsprechende nicht-kommerzielle Lizenz abgelaufen ist.
8947901E	Das Erstellungs- oder Installationsdatum der Schlüsseldatei ist fehlerhaft. Prüfen Sie das Systemdatum.
8947901F	Die Schlüsseldatei für eine Testlizenz kann nicht hinzugefügt werden, wenn bereits eine Testlizenz verwendet wird.
89479020	Die Denyliste der Schlüssel ist beschädigt oder fehlt.

89479021	Die Update-Beschreibung ist beschädigt oder fehlt.
89479022	Fehler in den Dienstdaten über den Lizenzschlüssel.
89479023	Eine ungültige Schlüsseldatei kann nicht verwendet werden, um einen Reserveschlüssel hinzuzufügen.
89479025	Fehler beim Senden der Anfrage an den Aktivierungsserver. Mögliche Gründe: Fehler bei der Internetverbindung oder vorübergehende Probleme auf dem Aktivierungsserver. Versuchen Sie, das Programm später mithilfe des Aktivierungscodes zu aktivieren. Sollte sich der Fehler wiederholen, wenden Sie sich bitte an Ihren Internetprovider.
89479026	Fehler in der Antwort des Aktivierungsservers.
89479027	Der Status der Antwort kann nicht abgerufen werden.
89479028	Fehler beim Speichern einer temporären Datei.
89479029	Es wurde ein ungültiger Aktivierungscode angegeben oder das Systemdatum des Computers ist falsch eingestellt. Prüfen Sie das Systemdatum des Computers.
8947902A	Der Schlüssel passt nicht zu diesem Programm oder die Lizenz ist abgelaufen. Kaspersky Endpoint Security kann nicht mit einer Schlüsseldatei für ein anderes Programm aktiviert werden.
8947902B	Der Download der Schlüsseldatei ist fehlgeschlagen. Es wurde ein ungültiger Aktivierungscode angegeben.
8947902C	Der Aktivierungsserver hat den Fehler 400 zurückgegeben.
8947902D	Der Aktivierungsserver hat Fehler 401 zurückgegeben.
8947902E	Der Aktivierungsserver hat Fehler 403 zurückgegeben.
8947902F	Der Aktivierungsserver hat Fehler 404 zurückgegeben.
89479030	Der Aktivierungsserver hat Fehler 405 zurückgegeben.
89479031	Der Aktivierungsserver hat Fehler 406 zurückgegeben.
89479032	Auf dem Proxyserver ist eine Authentifizierung erforderlich. Bitte prüfen Sie die Netzwerkeinstellungen.
89479033	Zeitüberschreitung der Anfrage.
89479034	Der Aktivierungsserver hat Fehler 409 zurückgegeben.
89479035	Der Aktivierungsserver hat Fehler 410 zurückgegeben.
89479036	Der Aktivierungsserver hat Fehler 411 zurückgegeben.
89479037	Der Aktivierungsserver hat Fehler 412 zurückgegeben.
89479038	Der Aktivierungsserver hat Fehler 413 zurückgegeben.
89479039	Der Aktivierungsserver hat Fehler 414 zurückgegeben.
8947903A	Der Aktivierungsserver hat Fehler 415 zurückgegeben.
8947903C	Interner Serverfehler.
8947903D	Diese Funktion wird nicht unterstützt.
8947903E	Ungültige Antwort vom Gateway. Bitte prüfen Sie die Netzwerkeinstellungen.
8947903F	Der Dienst ist nicht verfügbar (Fehler HTTP 503).
89479040	Zeitüberschreitung der Antwort vom Gateway. Bitte prüfen Sie die Netzwerkeinstellungen.

89479041	Das Protokoll wird nicht vom Server unterstützt.
89479043	Unbekannter HTTP-Fehler.
89479044	Ungültige ID der Ressource.
89479046	Ungültige Adresse (URL).
89479047	Ungültiger Zielordner.
89479048	Fehler beim Zuteilen von Arbeitsspeicher.
89479049	Fehler beim Konvertieren von Einstellungen in ANSI-Zeile (url, folder, agent).
8947904A	Fehler beim Erstellen eines Arbeitsthreads.
8947904B	Der Arbeitsthread wurde bereits gestartet.
8947904C	Der Arbeitsthread wurde nicht gestartet.
8947904D	Die Schlüsseldatei wurde auf dem Aktivierungsserver nicht gefunden.
8947904E	Der Schlüssel wurde gesperrt.
8947904F	Interner Fehler auf dem Aktivierungsserver.
89479050	Unzureichende Daten in der Aktivierungsanfrage.
89479053	Der Lizenzschlüssel ist abgelaufen.
89479054	Das Systemdatum des Computers ist falsch eingestellt.
89479055	Die Testlizenz ist abgelaufen.
89479056	Die Lizenz ist abgelaufen.
89479057	Die mit diesem Code zulässige Anzahl der Programmaktivierungen wurde überschritten!
89479058	Beim Aktivierungsvorgang ist ein Systemfehler aufgetreten.
89479059	Ein Schlüssel für eine nicht-kommerzielle Lizenz kann nicht als Schlüssel für eine kommerzielle Lizenz verwendet werden.
8947905C	Ein Aktivierungscode ist erforderlich.
89479062	Die Verbindung mit dem Aktivierungsserver ist fehlgeschlagen.
89479064	Der Aktivierungsserver ist nicht verfügbar. Überprüfen Sie die Einstellungen der Internetverbindung und wiederholen Sie den Aktivierungsversuch.
89479065	Das Veröffentlichungsdatum der Programm-Datenbanken liegt nach dem Ablaufdatum der Lizenz.
89479066	Ein aktiver Schlüssel kann nicht durch einen abgelaufenen Schlüssel ersetzt werden.
89479067	Ein Reserveschlüssel kann nicht hinzugefügt werden, wenn er früher abläuft als die aktuelle Lizenz.
89479068	Es ist kein aktueller Abo-Schlüssel vorhanden.
8947906A	Ungültiger Aktivierungscode (abweichende Prüfsumme).
8947906B	Der Schlüssel ist bereits aktiv.
8947906C	Die Typen der Lizenzen, die dem aktiven Schlüssel und dem Reserveschlüssel entsprechen, sind unterschiedlich.
8947906D	Die Lizenz unterstützt diese Komponente nicht.
8947906E	Ein Abo-Schlüssel kann nicht als Reserveschlüssel hinzugefügt werden.

89479213	Allgemeiner Fehler auf Transportebene.
89479214	Es konnte keine Verbindung mit dem Aktivierungsserver hergestellt werden.
89479215	Die Webadresse hat ein ungültiges Format.
89479216	Die Adresse des Proxyservers konnte nicht konvertiert werden.
89479217	Die Adresse des Servers konnte nicht konvertiert werden. Überprüfen Sie die Einstellungen der Internetverbindung.
89479218	Es konnte keine Verbindung mit dem Aktivierungsserver oder Proxyserver hergestellt werden.
89479219	Der Remote-Zugriff wurde verweigert.
8947921A	Zeitüberschreitung der Antwort.
8947921B	Fehler beim Senden einer HTTP-Anfrage.
8947921C	Fehler beim Herstellen einer SSL-Verbindung.
8947921D	Der Vorgang wurde wegen eines Rückrufs abgebrochen.
8947921E	Zu viele Umleitungen.
8947921F	Die Überprüfung des Empfängers ist fehlgeschlagen.
89479220	Leere Antwort des Aktivierungsservers.
89479221	Fehler beim Senden von Daten.
89479222	Fehler beim Datenempfang.
89479223	Fehler im lokalen SSL-Zertifikat.
89479224	Fehler bei der SSL-Verschlüsselung.
89479225	Fehler im SSL-Zertifikat des Servers.
89479226	Der Inhalt des Netzwerkpakets ist ungültig.
89479227	Der Zugriff wurde dem Benutzer verweigert.
89479228	Ungültige Datei des SSL-Zertifikats.
89479229	Es konnte keine SSL-Verbindung hergestellt werden.
8947922A	Ein Netzwerkpaket konnte nicht gesendet oder empfangen werden. Versuchen Sie es später erneut.
8947922B	Die Datei mit den zurückgerufenen Zertifikaten ist ungültig.
8947922C	Fehler in der Anfrage des SSL-Zertifikats.
89479401	Unbekannter Serverfehler.
89479402	Interner Serverfehler.
89479403	Für den eingegebenen Aktivierungscode ist kein Lizenzschlüssel vorhanden.
89479404	Der aktive Schlüssel wurde gesperrt.
89479405	Es fehlen obligatorische Parameter in der Anfrage für die Programmaktivierung.
89479406	Ungültiger Benutzername oder ungültiges Kennwort.
89479407	Auf den Server wurde ein ungültiger Aktivierungscode übertragen.
89479408	Der Aktivierungscode passt nicht zu Kaspersky Endpoint Security. Kaspersky Endpoint Security kann nicht mit einer Schlüsseldatei für ein unbekanntes Programm aktiviert werden.

89479409	In der Anfrage fehlt ein Aktivierungscode.
8947940B	Die Lizenz ist abgelaufen (nach Angaben des Aktivierungsservers).
8947940C	Das Programm wurde zu oft mit diesem Aktivierungscode aktiviert.
8947940D	Die Anfrage-ID besitzt ein ungültiges Format.
8947940E	Der Aktivierungscode passt nicht zu Kaspersky Endpoint Security. Der Aktivierungscode ist für ein anderes Kaspersky-Programm vorgesehen.
8947940F	Der Lizenzschlüssel kann nicht aktualisiert werden.
89479410	Der Aktivierungscode passt nicht zu dieser Region.
89479411	Der Aktivierungscode passt nicht zu dieser Sprachversion von Kaspersky Endpoint Security.
89479412	Eine zusätzliche Anfrage an den Aktivierungsserver ist erforderlich.
89479413	Der Aktivierungsserver hat Fehler 643 zurückgegeben.
89479414	Der Aktivierungsserver hat Fehler 644 zurückgegeben.
89479415	Der Aktivierungsserver hat Fehler 645 zurückgegeben.
89479416	Der Aktivierungsserver hat Fehler 646 zurückgegeben.
89479417	Das Format des Aktivierungscodes wird vom Aktivierungsserver nicht unterstützt.
89479418	Der Aktivierungscode besitzt ein ungültiges Format.
89479419	Die Systemzeit des Computers ist falsch eingestellt.
8947941A	Der Aktivierungscode passt nicht zu dieser Version von Kaspersky Endpoint Security.
8947941B	Das Abonnement ist abgelaufen.
8947941C	Für diesen Lizenzschlüssel wurde die maximale Anzahl der Aktivierungen überschritten.
8947941D	Ungültige digitale Signatur des Lizenzschlüssels.
8947941E	Zusätzliche Benutzerdaten sind erforderlich.
8947941F	Die Überprüfung der Benutzerdaten ist fehlgeschlagen.
89479420	Das Abonnement ist nicht aktiv.
89479421	Wartungsarbeiten auf dem Aktivierungsserver.
89479501	Unbekannter Fehler in Kaspersky Endpoint Security.
89479502	Eine ungültige Einstellung wurde übertragen (Beispiel: leere Adressliste für die Aktivierungsserver).
89479503	Ungültiger Aktivierungscode.
89479504	Ungültiger Benutzername.
89479505	Ungültiges Benutzerkennwort.
89479506	Der Aktivierungsserver hat eine falsche Antwort zurückgegeben.
89479507	Die Aktivierungsanfrage wurde unterbrochen.
89479509	Der Aktivierungsserver hat eine leere Weiterleitungsliste zurückgegeben.

Anhang. Programmprofile

Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Profile, die zur Programmverwaltung über die Befehlszeile vorgesehen sind. Sie können Profile für die Ausführung der Befehle `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` und `IMPORT` verwenden. Mithilfe von Profilen können Sie Programmeinstellungen anpassen (z. B. `STOP DeviceControl`) oder eine Aufgabe starten (z. B. `START Scan_My_Computer`).

Folgende Profile sind verfügbar:

- `AdaptiveAnomaliesControl` – Adaptive Kontrolle von Anomalien.
- `AMSI` – AMSI-Schutz.
- `BehaviorDetection` – Verhaltensanalyse.
- `DeviceControl` – Gerätekontrolle.
- `EntAppControl` – Programmkontrolle.
- `File_Monitoring` oder `FM` – Schutz vor bedrohlichen Dateien.
- `Firewall` oder `FW` – Firewall.
- `HIPS` – Programm-Überwachung.
- `IDS` – Schutz vor Netzwerkbedrohungen.
- `IntegrityCheck` – Integritätsprüfung.
- `Mail_Monitoring` oder `EM` – Schutz vor E-Mail-Bedrohungen.
- `Rollback` – Update-Rollback.
- `Scan_ContextScan` – Untersuchung aus dem Kontextmenü.
- `Scan_IdleScan` – Untersuchung im Hintergrund.
- `Scan_Memory` – Untersuchung des Arbeitsspeichers des Kerns.
- `Scan_My_Computer` – Vollständige Untersuchung.
- `Scan_Objects` – Benutzerdefinierte Untersuchung.
- `Scan_Qscan` – Untersuchung von Objekten, die beim Hochfahren des Betriebssystems geladen werden.
- `Scan_Removable_Drive` – Untersuchung von Wechseldatenträgern.
- `Scan_Startup` oder `STARTUP` – Untersuchung wichtiger Bereiche.
- `Updater` – Update.

- `Web_Monitoring` oder `WM` – Schutz vor Web-Bedrohungen.
- `WebControl` – Web-Kontrolle.

Außerdem unterstützt Kaspersky Endpoint Security auch die Verwendung von Dienstprofilen. Dienstprofile können erforderlich sein, wenn Sie sich an den Technischen Support von Kaspersky wenden.

Programmverwaltung über eine REST API

Kaspersky Endpoint Security bietet die folgenden Möglichkeiten: Programmeinstellungen anpassen, Untersuchung und Update der Antiviren-Datenbanken starten, sowie andere Aufgaben mithilfe von Drittherstellers-Lösungen ausführen. Kaspersky Endpoint Security bietet eine entsprechende API. Die REST API für Kaspersky Endpoint Security verwendet das HTTP-Protokoll und bietet eine Auswahl von „Anfrage/Antwort"-Vorgängen. Das bedeutet, dass Sie Kaspersky Endpoint Security zwar über eine Drittherstellers-Lösung verwalten können, aber nicht über die lokale Programmoberfläche oder über die Verwaltungskonsole von Kaspersky Endpoint Security.

Für die Programmverwaltung über eine REST API muss Kaspersky Endpoint Security mit REST API-Unterstützung installiert werden. Der REST-Client und Kaspersky Endpoint Security müssen auf demselben Computer installiert sein.

So gewährleisten Sie eine sichere Interaktion zwischen Kaspersky Endpoint Security und dem REST-Client:

- Passen Sie den Schutz des REST-Clients vor unbefugtem Zugriff so an, wie es der REST-Client-Entwickler empfiehlt. Passen Sie den Schreibschutz für den REST-Client-Ordner mithilfe von DACL (Discretionary Access Control List) an.
- Um den REST-Client auszuführen, verwenden Sie ein separates Benutzerkonto mit Administratorrechten. Deaktivieren Sie für dieses Benutzerkonto die interaktive Anmeldung im System.

Die Programmverwaltung über eine REST API erfolgt über die Adresse http://127.0.0.1 oder http://localhost. Es ist nicht möglich, Kaspersky Endpoint Security per Fernzugriff über eine REST API zu verwalten.

ÖFFNEN SIE DIE REST-API-DOKUMENTATION

Programminstallation mit einer REST API

Für die Programmverwaltung über eine REST API muss Kaspersky Endpoint Security mit REST API-Unterstützung installiert werden. Wenn Sie Kaspersky Endpoint Security über eine REST API verwalten, kann das Programm nicht mithilfe von Kaspersky Security Center verwaltet werden.

Um Kaspersky Endpoint Security mit REST API-Unterstützung zu installieren, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security Version 11.2.0 oder höher befindet.
3. Installieren Sie Kaspersky Endpoint Security mit den folgenden Einstellungen:
   - `RESTAPI=1`
   - `RESTAPI_User=<Benutzername>`

     Benutzername für die Programmverwaltung über eine REST API. Geben Sie den Benutzernamen im Format `<DOMAIN>\<UserName>` an (z. B. `RESTAPI_User=COMPANY\Administrator`). Das Programm kann nur unter diesem Benutzerkonto über eine REST API verwaltet werden. Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen.
   - `RESTAPI_Port=<Port>`

     Port für den Datenaustausch. Optionale Einstellung. Standardmäßig ist Port 6782 ausgewählt.

- `AdminKitConnector=1`

  Programmverwaltung mithilfe von Administrationssystemen. Die Verwaltung ist standardmäßig erlaubt.

Sie können die Einstellungen für die Verwendung einer REST API auch mithilfe der Dateien setup.ini angeben.

Die Einstellungen für die Verwendung einer REST API können nur während der Programminstallation festgelegt werden. Die Einstellungen können nach der Programminstallation nicht geändert werden. Wenn Sie die Einstellungen ändern möchten, entfernen Sie Kaspersky Endpoint Security und installieren Sie das Programm mit neuen Einstellungen für die Verwendung der REST API neu.

Beispiel:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

Auf diese Weise können Sie das Programm über eine REST API verwalten. Um die Funktion zu überprüfen, öffnen Sie die Dokumentation für die REST API mithilfe einer GET-Anfrage.

Beispiel:

```
GET http://localhost:6782/kes/v1/api-docs
```

Verwendung einer API

Der Zugriff auf das Programm kann über eine REST API mithilfe des Kennwortschutzes nicht beschränkt werden. Beispielsweise ist es nicht möglich, die Deaktivierung des Schutzes über eine REST API zu verbieten. Sie können den „Kennwortschutz“ über eine REST API anpassen und den Zugriff der Benutzer auf das Programm über die lokale Schnittstelle beschränken.

Um das Programm über eine REST API zu verwalten, muss der REST-Client unter dem Benutzerkonto ausgeführt werden, das Sie bei der Installation des Programms mit REST API-Unterstützung erstellt haben. Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen.

ÖFFNEN SIE DIE REST-API-DOKUMENTATION

Die Programmverwaltung über eine REST API umfasst die folgenden Schritte:

1. Fordern Sie die aktuellen Werte der Programmeinstellungen an. Senden Sie dazu eine GET-Anfrage.

   Beispiel:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Das Programm sendet eine Antwort mit der Struktur und den Werten der Einstellungen. Kaspersky Endpoint Security unterstützt die Formate XML und JSON.

   Beispiel:

   ```
   {
   “action”: 0,
   “enableSystemProcessesMemoryProtection”: true,
   “enabled”: true
   }
   ```

3. Ändern Sie die Programmeinstellungen. Senden Sie dazu eine POST-Anfrage. Verwenden Sie die Struktur aus der Antwort auf Ihre GET-Anfrage.

   Beispiel:

   ```
   POST http://localhost:6782/kes/v1/settings/ExploitPrevention
   {
   “action”: 0,
   “enableSystemProcessesMemoryProtection”: false,
   “enabled”: true
   }
   ```

4. Das Programm übernimmt die Änderungen in den Einstellungen und sendet eine Antwort mit den Ergebnissen der Programmkonfiguration.

Informationsquellen zum Programm

Seite für Kaspersky Endpoint Security auf der Kaspersky-Webseite

Auf der Seite für Kaspersky Endpoint Security finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Die Seite für Kaspersky Endpoint Security enthält einen Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite über Kaspersky Endpoint Security in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt auf der Website des Technischen Supports.

Auf der Seite für Kaspersky Endpoint Security in der Wissensdatenbank finden Sie nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Endpoint Security können die Artikel auch andere Kaspersky-Programme betreffen. Die Wissensdatenbank bietet außerdem Neuigkeiten über den Technischen Support.

Diskussion über Kaspersky-Programme in der Benutzer-Community

Wenn Ihre Frage nicht dringend ist, können Sie sie mit den Experten von Kaspersky und mit anderen Anwendern in unserer Community diskutieren.

In der Community können Sie Themen ansehen, eigene Kommentare schreiben und neue Themen zur Diskussion stellen.

Kontaktaufnahme mit dem Technischen Support

Wenn Sie in der Dokumentation oder in den anderen Informationsquellen zu Kaspersky Endpoint Security keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support. Der Technische Support beantwortet Ihre Fragen zur Installation und Verwendung von Kaspersky Endpoint Security.

Kaspersky unterstützt Kaspersky Endpoint Security während des Lebenszyklus der Programms (siehe Seite zum Produktlebenszyklus). Bitte beachten Sie die Support-Regeln, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Über die Website des Technischen Supports
- mit einer Anfrage an den Technischen Support von Kaspersky aus dem Portal Kaspersky CompanyAccount

Nachdem Sie den Technischen Support von Kaspersky über ein Problem informiert haben, kann es sein, dass die Support-Mitarbeiter Sie auffordern, eine *Protokolldatei* zu erstellen. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Der Technische Support benötigt möglicherweise auch weitere Informationen zum Betriebssystem und den auf dem Computer laufenden Prozessen sowie genaue Verlaufsberichte zur Ausführung von Programmkomponenten.

Es kann sein, dass Sie von den Support-Experten dazu aufgefordert werden, die Programmeinstellungen zu Diagnosezwecken zu ändern.

- Funktionalität zur Ermittlung erweiterter Diagnoseinformationen aktivieren
- Vornehmen von Feineinstellungen für bestimmte Programmkomponenten. Diese Einstellungen sind nicht über die standardmäßige Benutzeroberfläche verfügbar.
- Einstellungen für die Speicherung von empfangenen Diagnose-Informationen ändern
- Anpassen von Einstellungen für das Abfangen und für die Speicherung des Netzwerkverkehrs

Alle Informationen, welche für die oben genannten Aktionen erforderlich sind (z. B. Reihenfolge der Schritte, Einstellungsänderungen, Konfigurationsdateien, Skripte, erweiterte Optionen für die Befehlszeile, Debug-Module und spezielle Dienstprogramme) werden Ihnen von den Support-Experten mitgeteilt. Sie erhalten außerdem Informationen über den Umfang der Daten, die im Rahmen der Fehlersuche empfangen werden. Die ermittelten erweiterten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Die ermittelten Daten werden nicht automatisch an Kaspersky geschickt.

Die oben genannten Aktionen dürfen nur unter Anleitung der Support-Experten ausgeführt werden. Wenn die Programmeinstellungen auf eine andere Weise geändert werden, als im Administratorhandbuch oder in den Anleitungen der Support-Experten beschrieben, so kann das Betriebssystem verlangsamt oder gestört werden, das Schutzniveau des Computers sinken und der Zugriff auf und die Integrität von Informationen beschädigt werden.

Über die Zusammensetzung und Speicherung von Protokolldateien

Bis die erhaltenen Informationen an Kaspersky übertragen werden, sind Sie selbst verantwortlich für die Sicherheit der erhaltenen Informationen und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf die erhaltenen Informationen, die auf dem Computer gespeichert sind.

Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird.

Ablaufverfolgungsdateien werden gespeichert im Ordner %ProgramData%\Kaspersky Lab\KES\Traces. Eine Ausnahme bilden die Ablaufverfolgungsdateien des Authentifizierungsagenten.

Ablaufverfolgungsdateien werden nach folgendem Muster benannt: `KES<Versionsnummer des Dienstes_DatumXX.XX_UhrzeitXX.XX_pidXXX.><Typ der Protokolldatei>.log`.

Sie können die Daten einsehen, die in Protokolldateien aufgezeichnet wurden.

Alle Protokolldateien enthalten folgende allgemeinen Daten:

- Ereigniszeitpunkt
- Thread-Nummer

  Diese Informationen sind nicht in der Protokolldatei des Authentifizierungsagenten enthalten.

- Programmkomponente, auf die das Ereignis zurückgeht.
- Ereigniskategorie (informativ, Warnung, kritisch, Fehler)
- Ereignisbeschreibung für den Befehl der Programmkomponente und das Ausführungsergebnis für diesen Befehl

Kaspersky Endpoint Security speichert die Benutzerkennwörter nur in verschlüsselter Form in einer Ablaufverfolgungsdatei.

Inhalt der Protokolldateien SRV.log, GUI.log und ALL.log

In den Protokolldateien `SRV.log`, `GUI.log` und `ALL.log` können neben allgemeinen Daten auch die folgenden Informationen aufgezeichnet werden:

- Persönliche Daten wie Nachname und Vorname, falls diese Daten Bestandteil eines Dateipfads auf dem lokalen Computer sind.
- Daten über die Hardware, die auf dem Computer installiert ist (z. B. Daten über die BIOS/UEFI-Firmware). Diese Daten werden in einer Ablaufverfolgungsdatei aufgezeichnet, wenn die vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung ausgeführt wird.
- Benutzername und Kennwort, falls diese im Klartext übertragen wurden. Diese Daten können bei der Untersuchung des Internet-Datenverkehrs in den Protokolldateien gespeichert werden.
- Benutzername und Kennwort, falls diese in HTTP-Kopfzeilen enthalten sind.
- Benutzername für die Anmeldung bei Microsoft Windows, falls der Name des Benutzerkontos Bestandteil eines Dateinamens ist.

- Ihre E-Mail-Adresse oder Webadresse mit Benutzername und Kennwort, falls diese im Namen eines gefundenen Objekts enthalten sind.
- Webseiten, die Sie besuchen, sowie Links von diesen Webseiten. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm Webseiten untersucht.
- Adresse des Proxyservers, Computername, Port, IP-Adresse, Benutzername, der bei der Autorisierung auf dem Proxyserver verwendet wird. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm einen Proxyserver verwendet.
- Externe IP-Adressen, mit denen eine Verbindung zu Ihrem Computer aufgebaut wurde
- Nachrichtenbetreff, ID, Name des Absenders und Webadresse des Nachrichtenabsenders in einem sozialen Netzwerk Diese Daten werden in Protokolldateien aufgezeichnet, wenn die Komponente „Web-Kontrolle“ aktiviert ist.
- Daten über den Netzwerkverkehr. Diese Daten werden in einer Ablaufverfolgungsdatei aufgezeichnet, wenn die Komponenten zur Überwachung des Datenverkehrs aktiviert sind (z. B. „Web-Kontrolle“).
- Daten, die von den Kaspersky-Servern stammen (z. B. Version der Antiviren-Datenbanken).
- Status der Komponenten von Kaspersky Endpoint Security und Angaben über die Verwendung dieser Komponenten.
- Daten über die Aktionen, die der Benutzer mit dem Programm ausführt.
- Ereignisse des Betriebssystems.

Inhalt der Ablaufverfolgungsdateien HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Die Protokolldatei `HST.log` enthält neben allgemeinen Daten auch Informationen zur Ausführung der Update-Aufgabe für die Datenbanken und Programm-Module.

Die Protokolldatei `BL.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Programm auftreten, sowie Daten, die im Programm zur Problembehebung benötigt werden. Diese Datei wird erstellt, wenn das Programm mit dem Parameter avp.exe –bl gestartet wird.

Die Protokolldatei `Dumpwriter.log` enthält neben allgemeinen Daten auch Verwaltungsinformationen, die zur Behebung von Problemen benötigt werden, die bei der Protokollierung einer Dump-Datei des Programms auftreten.

Die Protokolldatei `WD.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Dienst avpsus auftreten. Dazu zählen auch Ereignisse über das Update der Programm-Module.

Die Protokolldatei `AVPCon.dll.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Modul auftreten, das für die Verbindung mit Kaspersky Security Center dient.

Inhalt von Ablaufverfolgungsdateien der Leistung

Ablaufverfolgungsdateien der Leistung werden nach folgendem Muster benannt:
`KES<Versionsnummer_DatumXX.XX_UhrzeitXX.XX_pidXXX.>PERF.HAND.etl`.

Ablaufverfolgungsdateien der Leistung enthalten neben allgemeinen Daten auch Informationen über die Prozessauslastung, über die Bootdauer des Betriebssystems und über aktive Prozesse.

Inhalt der Ablaufverfolgungsdatei der AMSI-Schutzkomponente

Die Protokolldatei AMSI.log enthält neben allgemeinen Daten auch Informationen über die Ergebnisse von Untersuchungen, die von Drittanbieter-Anwendungen angefordert wurden.

Inhalt der Ablaufverfolgungsdatei für die Komponente „Schutz vor E-Mail-Bedrohungen"

Die Ablaufverfolgungsdatei `mcou.OUTLOOK.EXE.log` kann neben allgemeinen Daten auch Bestandteile von E-Mail-Nachrichten enthalten, darunter auch E-Mail-Adressen.

Inhalt der Ablaufverfolgungsdatei für die Komponente „Untersuchung aus dem Kontextmenü"

Die Ablaufverfolgungsdatei `shellex.dll.log` enthält neben allgemeinen Daten auch Informationen über die Ausführung einer Untersuchungsaufgabe und Daten, die zur Behebung von Programmstörungen erforderlich sind.

Inhalt der Ablaufverfolgungsdateien für die Web-Plug-ins des Programms

Ablaufverfolgungsdateien des Programm-Web-Plug-ins werden auf dem Computer gespeichert, auf dem Kaspersky Security Center 12 Web Console bereitgestellt wurde, im Ordner Program Files\Kaspersky Lab\Kaspersky Lab Security Center Web Console 12\logs.

Die Ablaufverfolgungsdateien des Programm-Web-Plug-ins werden nach folgendem Muster benannt: `logs-kes_windows-<Typ der Ablaufverfolgungsdatei>.DESKTOP-<Aktualisierungsdatum der Datei>.log`. Web Console startet die Protokollierung nach der Installation und löscht die Ablaufverfolgungsdateien nach der Deinstallation von Web Console.

Die Ablaufverfolgungsdateien für das Web-Plug-in des Programms enthalten neben allgemeinen Daten auch folgende Informationen:

- Kennwort des Benutzers KLAdmin für die Entsperrung der Benutzeroberfläche von Kaspersky Endpoint Security (Kennwortschutz).
- Temporäres Kennwort zur Entsperrung der Benutzeroberfläche von Kaspersky Endpoint Security (Kennwortschutz).
- Benutzername und Kennwort für den SMTP-Mail-Server (E-Mail-Benachrichtigungen).
- Benutzername und Kennwort für den Proxyserver im Internet (Proxyserver).
- Benutzername und Kennwort für die Aufgabe *Auswahl der Programmkomponenten ändern*.
- Anmeldedaten und Pfade, die in den Richtlinieneigenschaften und in den Aufgaben von Kaspersky Endpoint Security angegeben sind.

Inhalt der Protokolldatei des Authentifizierungsagenten

Die Ablaufverfolgungsdatei des Authentifizierungsagenten wird im Ordner System Volume Information gespeichert und wird nach folgendem Muster benannt `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Die Protokolldatei des Authentifizierungsagenten enthält neben allgemeinen Daten auch Informationen über die Funktion des Authentifizierungsagenten und über Aktionen, die der Benutzer im Authentifizierungsagenten ausführt.

Ablaufverfolgung des Programms

Ablaufverfolgung des Programms bedeutet die ausführliche Aufzeichnung von Aktionen, die vom Programm ausgeführt werden, sowie von Mitteilungen über Ereignisse, die bei der Programmausführung eintreten.

Die Ablaufverfolgung des Programms darf nur unter Anleitung des Technischen Supports von Kaspersky ausgeführt werden.

Um eine Ablaufverfolgungsdatei über das Programm zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

   Das Fenster **Support** wird geöffnet.

2. Klicken Sie im Fenster **Support** auf die Schaltfläche **Support Tools**.

3. Verwenden Sie den Schalter **Ablaufverfolgung des Programms aktivieren**, um die Protokollierung der Programmabläufe zu aktivieren oder zu deaktivieren.

4. Wählen Sie in der Dropdown-Liste **Protokollierung von Ereignissen** einen Modus für die Ablaufverfolgung des Programms aus:

   - **Mit Rotation**. Protokollierungsergebnisse in einer beschränkten Anzahl von Dateien mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird. Wenn dieser Modus ausgewählt ist, können Sie die maximale Anzahl von Dateien für die Rotation und die maximale Größe für jede Datei festlegen.

   - **In eine Einzeldatei schreiben**. Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).

5. Wählen Sie in der Dropdown-Liste **Stufe** die Protokollierungsstufe.

   Es wird empfohlen, die Support-Experten nach der erforderlichen Protokollierungsstufe zu fragen. Es wird empfohlen, die Stufe **Normal (500)** einzustellen, wenn keine Support-Empfehlungen für die Protokollierungsstufe vorliegen.

6. Starten Sie Kaspersky Endpoint Security neu.

7. Um die Ablaufverfolgung zu stoppen, kehren Sie zum Fenster **Support** zurück und deaktivieren Sie die Ablaufverfolgung.

Sie können auch Ablaufverfolgungsdateien erstellen, während Sie das Programm aus der Befehlszeile installieren. Dies ist auch mithilfe der Datei setup.ini möglich.

Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird. Ablaufverfolgungsdateien werden gespeichert im Ordner %ProgramData%\Kaspersky Lab\KES\Traces. Eine Ausnahme bilden die Ablaufverfolgungsdateien des Authentifizierungsagenten. Die Protokollierung ist standardmäßig deaktiviert.

Ablaufverfolgung der Programmleistung

Kaspersky Endpoint Security erlaubt es, Informationen über Probleme zu erhalten, die im Computer bei der Programmverwendung auftreten. Sie können beispielsweise Informationen darüber erhalten, ob sich nach der Programminstallation das Hochfahren des Betriebssystems verzögert. Dazu erstellt Kaspersky Endpoint Security Ablaufverfolgungsdateien der Leistung. Bei der *Ablaufverfolgung der Leistung* werden vom Programm ausgeführte Aktionen protokolliert, um Leistungsprobleme von Kaspersky Endpoint Security zu erkennen. Um Informationen zu empfangen, verwendet Kaspersky Endpoint Security die Windows-Ereignisverfolgung (ETW – Event Tracing for Windows). Die Funktionsdiagnose für Kaspersky Endpoint Security und die Ermittlung der Problemursachen erfolgt durch den Technischen Support von Kaspersky.

Die Ablaufverfolgung des Programms darf nur unter Anleitung des Technischen Supports von Kaspersky ausgeführt werden.

Um eine Ablaufverfolgungsdatei über die Leistung zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

   Das Fenster **Support** wird geöffnet.

2. Klicken Sie im Fenster **Support** auf die Schaltfläche **Support Tools**.

3. Verwenden Sie den Schalter **Ablaufverfolgung der Leistung aktivieren**, um die Protokollierung der Programmleistung zu aktivieren oder zu deaktivieren.

4. Wählen Sie in der Dropdown-Liste **Protokollierung von Ereignissen** einen Modus für die Ablaufverfolgung des Programms aus:

   - **Mit Rotation**. Protokollierungsergebnisse in einer beschränkten Anzahl von Dateien mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird. Wenn dieser Modus ausgewählt ist, können Sie die maximale Größe für jede Datei festlegen.

   - **In eine Einzeldatei schreiben**. Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).

5. Wählen Sie in der Dropdown-Liste **Stufe** ein Ablaufverfolgungsstufe aus:

   - **Oberflächlich**. Kaspersky Endpoint Security analysiert die wichtigsten Prozesse des Betriebssystems, die mit der Leistung zusammenhängen.

   - **Detailliert.** Kaspersky Endpoint Security analysiert alle Prozesse des Betriebssystems, die mit der Leistung zusammenhängen.

6. Wählen Sie in der Dropdown-Liste **Protokollierungstyp** einen Ablaufverfolgungstyp aus:

   - **Basisinformationen**. Kaspersky Endpoint Security analysiert die Prozesse, während das Betriebssystem läuft. Verwenden Sie diesen Ablaufverfolgungstyp, wenn ein Problem nach dem Systemstart reproduziert wird, z. B. ein Problem beim Internetzugriff im Browser.

   - **Beim Neustart**. Kaspersky Endpoint Security analysiert die Prozesse nur beim Systemstart. Nach dem Systemstart beendet Kaspersky Endpoint Security die Ablaufverfolgung. Verwenden Sie diesen Ablaufverfolgungstyp, wenn das Problem mit einer Verzögerung des Systemstarts zusammenhängt.

7. Starten Sie den Computer neu und reproduzieren Sie das Problem.

8. Um die Ablaufverfolgung zu stoppen, kehren Sie zum Fenster **Support** zurück und deaktivieren Sie die Ablaufverfolgung.

Dadurch wird im Ordner %ProgramData%\Kaspersky Lab eine Ablaufverfolgungsdatei über die Leistung erstellt. Senden Sie die erstellte Ablaufverfolgungsdatei an den Technischen Support von Kaspersky.

Aufzeichnung von Dump-Dateien

Eine Dump-Datei enthält alle Informationen über den Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt, als diese Dump-Datei erstellt wurde.

Gespeicherte Dump-Dateien können vertrauliche Daten enthalten. Sie müssen selbst für den Schutz der Dump-Dateien sorgen, um die Kontrolle des Zugriffs auf die Daten zu gewährleisten.

Dump-Dateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden unwiderruflich gelöscht, wenn das Programm entfernt wird. Dump-Dateien werden im Ordner %ProgramData%\Kaspersky Lab gespeichert.

Um die Dump-Aufzeichnung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Dump-Aufzeichnung aktivieren**, um das Schreiben von Dump-Dateien zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Schutz von Dump- und Protokolldateien

Dump-Dateien und Protokolldateien enthalten Informationen über das Betriebssystem und können Benutzerdaten enthalten. Um einen unberechtigten Zugriff auf diese Daten zu verhindern, können Sie den Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren.

Wenn der Schutz für Dump-Dateien und Protokolldateien aktiviert ist, besitzen folgende Benutzer Zugriff auf die Dateien:

- Zugriff auf Dump-Dateien besitzen der Systemadministrator, der lokale Administrator und der Benutzer, der die Aufzeichnung von Dump-Dateien und Protokolldateien aktiviert hat.
- Zugriff auf Protokolldateien besitzen nur der Systemadministrator und der lokale Administrator.

Um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie unten im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster Programmeinstellungen den Abschnitt **Allgemein**.
3. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Dateischutz zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Dump-Dateien und Protokolldateien, die bei aktiviertem Schutz aufgezeichnet wurden, bleiben nach dem Ausschalten dieser Funktion geschützt.

Einschränkungen und Warnungen

Kaspersky Endpoint Security besitzt eine Reihe von nicht kritischen Einschränkungen.

Programm installieren

- Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10, Microsoft Windows Server 2016 und Microsoft Windows Server 2019 finden Sie in der Wissensdatenbank des Technischen Supports.

- Nachdem das Programm auf einem infizierten Computer installiert wurde, informiert es den Benutzer nicht über die Notwendigkeit, eine Computeruntersuchung durchzuführen. Bei der Aktivierung des Programms können Probleme auftreten. Um diese Probleme zu lösen, starten Sie eine Untersuchung wichtiger Bereiche.

- Wenn in den Dateien setup.ini und setup.reg Nicht-ASCII-Zeichen (z. B. russische Buchstaben) verwendet werden, wird empfohlen, die Datei mit notepad.exe zu bearbeiten und die Datei in UTF-16LE-Kodierung zu speichern. Andere Kodierungen werden nicht unterstützt.

- Das Programm unterstützt nicht die Verwendung von Nicht-ASCII-Zeichen bei der Angabe des Programminstallationspfads in den Einstellungen des Installationspakets.

- Wenn Programmeinstellungen aus einer CFG-Datei importiert werden, wird der Wert der Einstellung, die die Teilnahme am Kaspersky Security Network definiert, nicht übernommen. Bitte lesen Sie nach dem Import der Einstellungen den Text der Erklärung zum Kaspersky Security Network und bestätigen Sie Ihr Einverständnis zur Teilnahme am Kaspersky Security Network. Sie können den Text der Erklärung in der Programmoberfläche oder in der Datei ksn_*.txt lesen, die sich in dem Ordner befindet, der das Programmverteilungskit enthält.

- Beim Upgrade von Kaspersky Endpoint Security 10 Service Pack 2 für Windows (Build 10.3.0.6294) wird die Programm-Überwachung-Komponente aktiviert.

- Bei einem Upgrade von Kaspersky Endpoint Security 10 für Windows Service Pack 2 (Build 10.3.0.6294) werden die Dateien, die in der älteren Programmversion ins Backup und in die Quarantäne verschoben wurden, in das Backup der neuen Programmversion übertragen. Diese Dateien werden für ältere Versionen als Kaspersky Endpoint Security 10 für Windows Service Pack 2 (Build 10.3.0.6294) nicht übertragen. Um sie zu speichern, müssen Sie die Dateien aus der Quarantäne und der Datensicherung vor dem Upgrade des Programms wiederherstellen. Nachdem das Upgrade abgeschlossen ist, überwachen Sie die wiederhergestellten Dateien erneut.

- Wenn Sie die Verschlüsselung (FLE oder FDE) oder die Gerätekontrolle-Komponente entfernen und dann neu installieren möchten, müssen Sie das System vor der Neuinstallation neu starten.

- Wenn Sie das Betriebssystem Microsoft Windows 10 verwenden, müssen Sie das System neu starten, nachdem Sie die Komponente File Level Encryption (FLE) entfernt haben.

- Wenn Sie versuchen, eine beliebige Version des AES-Verschlüsselungsmoduls auf einem Computer zu installieren, auf dem Kaspersky Endpoint Security für Windows 11.6.0 ist, aber keine Verschlüsselungskomponenten installiert sind, wird die Installation des Verschlüsselungsmoduls mit einer Fehlermeldung beendet, die besagt, dass eine neuere Version des Programms installiert ist. Beginnend mit Kaspersky Endpoint Security 10 für Windows Service Pack 2 (Version 10.3.0.6294) gibt es keine separate Installationsdatei für das Verschlüsselungsmodul. Verschlüsselungsbibliotheken sind im Verteilungspaket des Programms enthalten. Kaspersky Endpoint Security 11.6.0 ist mit AES-Verschlüsselungsmodulen inkompatibel. Die für die Verschlüsselung erforderlichen Bibliotheken werden automatisch installiert, wenn die Komponente „Full Disk Encryption“ (FDE) oder „File Level Encryption“ (FLE) ausgewählt wird.

- Die Installation des Programms kann mit einem Fehler enden, der besagt, dass *ein Programm, dessen Name fehlt oder nicht lesbar ist, auf Ihrem Computer installiert ist*. Das bedeutet, dass inkompatible Programme oder Fragmente davon auf Ihrem Computer verbleiben. Um Artefakte von inkompatiblen Programmen zu entfernen, senden Sie eine Anfrage mit einer detaillierten Beschreibung der Situation über Kaspersky CompanyAccount an den technischen Support von Kaspersky.

- Ab Programmversion 11.0.0 können Sie das MMC-Plug-in für Kaspersky Endpoint Security für Windows über die vorherige Plug-in-Version installieren. Um zur vorherigen Plug-in-Version zurückzukehren, löschen Sie das aktuelle Plug-in und installieren Sie eine ältere Version des Plug-ins.

- Beim Upgrade von Kaspersky Endpoint Security 11.0.0 oder 11.0.1 für Windows werden die Einstellungen des Zeitplans für lokale Aufgaben für *Update*, *Untersuchung wichtiger Bereiche*, *Benutzerdefinierte Untersuchung* und *Integritätsprüfung* nicht gespeichert.

- Wenn Sie die Entfernung des Programms abgebrochen haben, starten Sie die Wiederherstellung nach dem Neustart des Computers.

- Auf Computern mit Windows 10 Version 1903 und 1909 können Upgrades von Kaspersky Endpoint Security 10 für Windows Service Pack 2 Maintenance Release 3 (Build 10.3.3.275), Service Pack 2 Maintenance Release 4 (Build 10.3.3.304), 11.0.0 und 11.0.1 mit installierter File Level Encryption (FLE)-Komponente mit einem Fehler enden. Dies liegt daran, dass die Dateiverschlüsselung für diese Versionen von Kaspersky Endpoint Security für Windows in Windows 10 Version 1903 und 1909 nicht unterstützt wird. Vor der Installation dieses Upgrades wird Ihnen empfohlen, die Dateiverschlüsselungskomponente zu entfernen.

- Wenn Sie eine frühere Version des Programms auf Version 11.6.0 aktualisieren, starten Sie zur Installation des Kaspersky Endpoint-Agenten den Computer neu und melden Sie sich mit einem Konto mit lokalen Administratorrechten beim System an. Andernfalls wird der Kaspersky Endpoint Agent während des Upgrade-Vorgangs nicht installiert.

- Wenn das Programm nicht erfolgreich mit der in einem Serverbetriebssystem ausgewählten Komponente des Kaspersky Endpoint Agent installiert wird und das Fenster *Fehler im Windows Installer Coordinator* erscheint, lesen Sie die Anweisungen auf der Support-Website von Microsoft.

- Wenn das Programm lokal im nicht-interaktiven Modus installiert wurde, verwenden Sie die mitgelieferte setup.ini-Datei, um die installierten Komponenten zu ersetzen.

- Wenn Sie Kaspersky Endpoint Security 10 für Windows Service Pack 2 Maintenance Release 4 mit der installierten Komponente „Verschlüsselung von Dateien“ (FLE) auf Computern mit Windows 10 Version 1809, 1903 und 1909 upgraden, werden die FDE-Treiber nicht auf das WinRE-Abbild installiert.

- Nachdem Kaspersky Endpoint Security für Windows in einigen Konfigurationen von Windows 7 installiert wurde, funktioniert Windows Defender weiterhin. Es wird empfohlen, Windows Defender manuell zu deaktivieren, um eine Beeinträchtigung der Systemleistung zu verhindern.

- Nachdem das Programm von Versionen vor Kaspersky Endpoint Security 11 für Windows aktualisiert wurde, muss der Computer neu gestartet werden.

Unterstützung für virtuelle Plattformen

- Das Dateisystem ReFS wird nur eingeschränkt unterstützt:
  - Nachdem die Virenuntersuchung eines Servers gestartet wurde, werden die mit iChecker hinzugefügten Untersuchungsausnahmen beim Server-Neustart zurückgesetzt.
  - Kaspersky Endpoint Security erkennt die Dateien eicar.com und susp-eicar.com nicht, wenn auf dem Computer die Datei meicar.exe vorhanden war, bevor Kaspersky Endpoint Security installiert wurde.
- Die Konfigurationen Server Core und Cluster Mode werden nicht unterstützt.
- Die Technologien „Verschlüsselung von Dateien“ (FLE) und „Kaspersky-Festplattenverschlüsselung“ (FDE) werden auf Server-Plattformen nicht unterstützt.
- Die „Gerätekontrolle“ wird auf Serverplattformen nicht unterstützt.
- Microsoft Windows Server 2008 wurde von der Unterstützung ausgeschlossen. - Die Programminstallation auf einem Computer mit dem Betriebssystem Microsoft Windows Server 2008 wird nicht unterstützt.
- Wenn Sie mehrere Arbeitssitzungen auf dem Terminalserver gestartet haben, funktionieren die Benachrichtigungen von Kaspersky Endpoint Security möglicherweise nicht korrekt. Beispiel: Der Benutzer der Sitzung Nr. 1 startet die Überprüfung der Reputation einer Datei in KSN. Kaspersky Endpoint Security zeigt dem Benutzer der Sitzung Nr. 2 eine Benachrichtigung mit den Ergebnissen der Überprüfung an.

Unterstützte virtuelle Plattformen:

- Full Disk Encryption (FDE) wird auf virtuellen Hyper-V-Maschinen nicht unterstützt.
- Full Disk Encryption (FDE) wird auf virtuellen Citrix-Plattformen nicht unterstützt.
- Die multisessionfähige Version von Windows 10 Enterprise wird mit Einschränkungen unterstützt:
  - Kaspersky Endpoint Security betrachtet das multisessionfähige Windows 10 Enterprise als ein Server-Betriebssystem. Darum wird das multisessionfähige Windows 10 Enterprise mit den für Server-Plattformen spezifischen Einschränkungen unterstützt. Beispielsweise können Server bestimmte Komponenten von Kaspersky Endpoint Security nicht verwenden. Außerdem verwendet das Programm einen Server-Lizenzschlüssel anstatt eines Workstation-Lizenzschlüssels.
  - Die vollständige Festplattenverschlüsselung (FDE) wird nicht unterstützt.
  - Die Verwaltung von BitLocker wird nicht unterstützt.
  - Die Verwendung von Kaspersky Endpoint Security mit Wechseldatenträgern wird nicht unterstützt. Die Microsoft Azure-Infrastruktur definiert Wechseldatenträger als Netzlaufwerke.
- Die Installation und Verwendung von Verschlüsselung auf Dateiebene (FLE) wird auf virtuellen Citrix-Plattformen nicht unterstützt.
- Um die Kompatibilität von Kaspersky Endpoint Security für Windows mit Citrix PVS zu unterstützen, führen Sie die Installation mit aktivierter Option **Kompatibilität mit Citrix PVS gewährleisten** durch. Diese Option kann im Installationsassistenten oder durch Verwendung des Befehlszeilenparameters `/pCITRIXCOMPATIBILITY=1` aktiviert werden. Im Falle einer Ferninstallation muss die KUD-Datei durch Hinzufügen des folgenden Parameters bearbeitet werden: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Bevor Sie mit dem Klonen beginnen, müssen Sie den Selbstschutz-Mechanismus deaktivieren, um virtuelle Maschinen zu klonen, die vDisk verwenden.
- Wenn Sie einen Referenzcomputer für das Citrix XenDesktop-Master-Image mit vorinstalliertem Kaspersky Endpoint Security für Windows und dem Kaspersky Security Center Administrationsagenten vorbereiten, fügen Sie der Konfigurationsdatei die folgenden Arten von Ausnahmen hinzu:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Einzelheiten zu Citrix XenDesktop finden Sie auf der Support-Website von Citrix.
- In einigen Fällen kann der Versuch, einen Wechseldatenträger sicher zu trennen, bei einer virtuellen Maschine fehlschlagen, die auf einem VMware ESXi-Hypervisor bereitgestellt wird. Versuchen Sie noch einmal, das Gerät sicher zu trennen.

Kompatibilität mit Kaspersky Security Center

- Die Komponente „Adaptive Kontrolle von Anomalien“ können Sie nur in Kaspersky Security Center Version 11 oder höher verwalten.
- Der Bedrohungsbericht für Kaspersky Security Center 11 zeigt möglicherweise keine Informationen über die Maßnahmen an, die für durch den AMSI-Schutz erkannte Bedrohungen ergriffen wurden.
- Der Funktionsstatus für die Komponenten „AMSI-Schutz“ und „Adaptive Kontrolle von Anomalien“ ist nur in Kaspersky Security Center Version 11 oder höher verfügbar. Den Funktionsstatus können Sie anzeigen in der Konsole von Kaspersky Security Center in den Computereigenschaften im Abschnitt **Aufgaben**. Auch die Berichte für diese Komponenten sind nur in Kaspersky Security Center Version 11 oder höher verfügbar.

Lizenzverwaltung

- Wenn die Systemmeldung *Fehler beim Datenempfang* angezeigt wird, überprüfen Sie, ob der Computer, auf dem Sie die Aktivierung durchführen, über Netzwerkzugriff verfügt, oder konfigurieren Sie die Aktivierungseinstellungen über den Aktivierungs-Proxy von Kaspersky Security Center.
- Das Programm kann über Kaspersky Security Center nicht mit einem Abonnement aktiviert werden, wenn die Lizenz abgelaufen ist oder wenn auf dem Computer eine Testlizenz aktiv ist. Um eine Testlizenz oder eine Lizenz, die bald abläuft, durch eine Abonnementlizenz zu ersetzen, verwenden Sie die Aufgabe Lizenzverteilung.
- In der Programmoberfläche wird das Ablaufdatum der Lizenz in der lokalen Zeit des Computers angezeigt.
- Die Installation des Programms mit einer eingebetteten Schlüsseldatei auf einem Computer mit instabilem Internetzugang kann zur temporären Anzeige von Ereignissen führen, die besagen, dass das Programm nicht aktiviert ist oder dass die Lizenz den Betrieb der Komponente nicht zulässt. Dies liegt daran, dass das Programm zunächst die eingebettete Testlizenz installiert und zu aktivieren versucht, die für die Aktivierung während des Installationsvorgangs einen Internetzugang erfordert.
- Während des Testzeitraums kann die Installation eines Programm-Upgrades oder Patches auf einem Computer mit instabilem Internetzugang dazu führen, dass vorübergehend Ereignisse angezeigt werden, die besagen, dass das Programm nicht aktiviert ist. Dies liegt daran, dass das Programm die eingebettete Testlizenz, die bei der Installation eines Upgrades einen Internetzugang für die Aktivierung erfordert, erneut installiert und zu aktivieren versucht.
- Wenn die Testlizenz bei der Installation des Programms automatisch aktiviert und das Programm dann entfernt wurde, ohne die Lizenzinformationen zu speichern, wird das Programm bei einer Neuinstallation nicht automatisch mit der Testlizenz aktiviert. Aktivieren Sie in diesem Fall das Programm manuell.
- Wenn Sie Kaspersky Security Center Version 11 und Kaspersky Endpoint Security Version 11.6.0 verwenden, funktionieren die Berichte über die Komponentenleistung möglicherweise fehlerhaft. Wenn Sie Komponenten von Kaspersky Endpoint Security installiert haben, die nicht in Ihrer Lizenz enthalten sind, sendet der Administrationsagent möglicherweise Fehler über den Komponentenstatus an das Windows-Ereignisprotokoll. Um solche Fehler zu vermeiden, entfernen Sie die Komponenten, die nicht in Ihrer Lizenz enthalten sind.

Rollback von schädlichen Aktionen

- Das Programm stellt Dateien nur auf Geräten mit dem Dateisystem NTFS und FAT32 wieder her.
- Das Programm stellt Dateien mit folgenden Erweiterungen wieder her: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Dateien, die sich auf Netzlaufwerken und wiederbeschreibbaren CD/DVD-Disks befinden, können nicht wiederhergestellt werden.
- Dateien, die mithilfe von Encryption File System (EFS) verschlüsselt wurden, können nicht wiederhergestellt werden. Details über die Funktion von EFS finden Sie auf der *Microsoft-Website*.
- Veränderungen von Dateien, die von Prozessen auf der Kernel-Ebene des Betriebssystems ausgeführt wurden, werden vom Programm nicht kontrolliert.
- Veränderungen von Dateien, die über eine Netzwerkschnittstelle ausgeführt wurden, werden vom Programm nicht kontrolliert. (Beispiel: Eine Datei wurde in einen gemeinsamen Ordner verschoben und der Prozess wurde per Fernzugriff von einem anderen Computer gestartet.)

Firewall

- Die Filterung von Paketen oder Verbindungen nach lokaler Adresse, physischer Schnittstelle und Paketlaufzeit (TTL) wird in den folgenden Fällen unterstützt:
  - Nach lokaler Adresse für ausgehende Pakete oder Verbindungen in Programmregeln für TCP und UDP und Paketregeln.
  - Nach lokaler Adresse für eingehende Pakete oder Verbindungen (außer UDP) in Blockierungsregeln für Anwendungen und Paketregeln.
  - Nach Paketlaufzeit (TTL) in Blockpaketregeln für eingehende oder ausgehende Pakete.
  - Nach Netzwerkschnittstelle für eingehende und ausgehende Pakete oder Verbindungen in Paketregeln.
- In den Programmversionen 11.0.0 und 11.0.1 werden definierte MAC-Adressen fälschlicherweise angewendet. Die MAC-Adresseinstellungen für die Versionen 11.0.0, 11.0.1 und 11.1.0 oder höher sind nicht kompatibel. Nach einem Upgrade des Programms oder des Plug-Ins von diesen Versionen auf Version 11.1.0 oder höher müssen Sie die definierten MAC-Adressen in den Firewall-Regeln überprüfen und neu konfigurieren.
- Beim Upgrade des Programms von den Versionen 11.1.1 und 11.2.0 auf Version 11.6.0 werden die Berechtigungsstatus für die folgenden Firewall-Regeln nicht migriert:
  - Anfragen an DNS-Server über TCP.
  - Anfragen an DNS-Server über UDP.
  - Jede Netzwerkaktivität.
  - ICMP Destination unerreichbar für eingehende Antworten.
  - Eingehender ICMP-Stream.
- Wenn Sie ein Netzwerkadapter oder eine Paket-Lebensdauer (TTL) für eine Paket-Erlaubnisregel konfiguriert haben, hat diese Regel eine niedrigere Priorität als eine blockierende Programmregel. Mit anderen Worten: Wenn die Netzwerkaktivität für ein Programm blockiert ist (z. B. da das Programm zur Sicherheitsgruppe *Stark beschränkt* gehört), können Sie die Netzwerkaktivität des Programms erlauben, indem Sie eine Paketregel mit diesen Einstellungen verwenden. In allen übrigen Fällen hat eine Paketregel eine höhere Priorität als eine Netzwerkregel für Programme.
- Beim Import der Liste mit Firewall-Paketregeln kann in Kaspersky Endpoint Security für Windows 11.5.0–11.6.0 ein Fehler auftreten. Das kann dazu führen, dass benutzerdefinierte lokale oder Remote-Adressen aus einer Regel gelöscht werden. Wenden Sie sich bitte an den technischen Support, um diesen Fehler zu beheben. Der technische Support stellt Ihnen ein Update mit einem Patch für das Plug-in zur Verfügung. Alternativ können Sie das Programm nach der Veröffentlichung auf die nächste Version aktualisieren.
- Beim Import einer Liste mit Firewall-Paketregeln ändert Kaspersky Endpoint Security eventuell die Regelnamen. Das Programm erkennt Regeln mit dem gleichen Satz an Haupteinstellungen wie Protokoll, Richtung, Remote-Ports und lokale Ports sowie Paketlaufzeit (TTL). Haben mehrere Regeln das gleiche Set an Haupteinstellungen, so weist das Programm diesen Regeln den gleichen Namen zu oder versieht die Namen mit einem Einstellungstag. Kaspersky Endpoint Security importiert also alle Paketregeln, aber die Namen der Regeln mit gleichen Haupteinstellungen werden eventuell geändert.
- Wenn eine Netzwerkregel für Pakete in Kaspersky Endpoint Security 11.6.0 oder älter ausgelöst wird, zeigt die Spalte **Programmname** im Firewall-Bericht immer den Wert *Kaspersky Endpoint Security* an. Darüber hinaus blockiert die Firewall die Verbindung für alle Programme auf Paketebene. Dieses Verhalten wurde in Kaspersky Endpoint Security 11.7.0 und späteren Versionen verändert. Die Spalte **Regeltyp** wurde dem

Firewall-Bericht hinzugefügt. Wird eine Netzwerkregel für Pakete ausgelöst, so bleibt der Wert in der Spalte **Programmname** leer.

Programmkontrolle

- Bei der Arbeit in Microsoft Windows 10 im Denylist-Modus von Programmen können Blockierungsregeln falsch angewendet werden, was zur Blockierung von Programmen führen kann, die nicht in Regeln angegeben sind.
- Wenn progressive Webanwendungen (PWA) durch die Komponente Programmkontrolle blockiert werden, wird appManifest.xml im Bericht als das blockierte Programm angezeigt.

Gerätekontrolle

- Der Zugriff auf Druckergeräte, die der vertrauenswürdigen Liste hinzugefügt wurden, wird durch Geräte- und Bus-Blockierungsregeln blockiert.
- Bei MTP-Geräten wird die Steuerung von Lese-, Schreib- und Verbindungsvorgängen unterstützt, wenn Sie die integrierten Microsoft-Treiber des Betriebssystems verwenden. Wenn ein Benutzer einen benutzerdefinierten Treiber für die Arbeit mit einem Gerät installiert (z. B. als Teil von iTunes oder Android Debug Bridge), funktioniert die Kontrolle der Lese- und Schreibvorgänge möglicherweise nicht.
- Bei der Arbeit mit MTP-Geräten werden die Zugriffsregeln nach dem erneuten Anschließen des Geräts geändert.
- Wenn Sie der Liste der vertrauenswürdigen Geräte auf der Grundlage einer Modellmaske ein Gerät hinzufügen und Zeichen verwenden, die in der ID, aber nicht im Modellnamen enthalten sind, werden diese Geräte nicht hinzugefügt. Auf einer Workstation werden diese Geräte auf der Grundlage einer ID-Maske zur Liste der vertrauenswürdigen Geräte hinzugefügt.

Web-Kontrolle

- Die Formate OGV und WEBM werden nicht unterstützt.
- Das RTMP-Protokoll wird nicht unterstützt.

Adaptive Kontrolle von Anomalien

- Es wird empfohlen, Ausnahmen automatisch auf der Grundlage des Ereignisses zu erstellen. Wenn Sie eine Ausnahme manuell hinzufügen, fügen Sie bei der Angabe des Zielobjekts das Zeichen `*` am Anfang des Pfades ein.
- Ein Bericht über Regeln zur adaptiven Kontrolle von Anomalien kann nicht erstellt werden, wenn die Stichprobe auch nur ein Ereignis enthält, dessen Name mehr als 260 Zeichen enthält.
- Aus dem Abschnitt „Auslösen von Regeln“ der Datenverwaltung der Komponente „Adaptive Kontrolle von Anomalien“ können keine Ausnahmen hinzugefügt werden, wenn ein Objekt oder ein Prozess einen Wert hat, der aus über 256 Zeichen besteht (z. B. Pfad des Zielobjekts). Sie können eine Ausnahme manuell in den Richtlinieneinstellungen hinzufügen. Sie können eine Ausnahme auch im Bericht über die ausgelösten Regeln der Komponente „Adaptive Kontrolle von Anomalien“ hinzufügen.

Festplattenverschlüsselung (FDE)

- Nach der Installation des Programms müssen Sie das Betriebssystem neu starten, damit die Festplattenverschlüsselung ordnungsgemäß funktioniert.
- Der Authentifizierungsagent unterstützt keine Hieroglyphen oder die Sonderzeichen `|` und `\`.
- Damit der Computer nach der Verschlüsselung optimal funktioniert, muss der Prozessor den Befehlssatz AES-NI (Intel Advanced Encryption Standard New Instructions) unterstützen. Wenn der Prozessor den Befehlssatz AES-NI nicht unterstützt, kann die Leistung des Computers sinken.
- Wenn es Prozesse gibt, die versuchen, auf verschlüsselte Geräte zuzugreifen, bevor das Programm den Zugriff auf diese Geräte gewährt hat, zeigt das Programm eine Warnung an, die besagt, dass diese Prozesse beendet werden müssen. Wenn die Prozesse nicht beendet werden können, schließen Sie die verschlüsselten Geräte wieder an.
- Die eindeutigen IDs von Festplattenlaufwerken werden in der Geräteverschlüsselungsstatistik in invertiertem Format angezeigt.
- Es wird nicht empfohlen, Geräte zu formatieren, während sie verschlüsselt werden.
- Wenn mehrere Wechseldatenträger gleichzeitig an einem Computer angeschlossen sind, kann die Verschlüsselungsrichtlinie nur auf einen einzigen Wechseldatenträger angewendet werden. Wenn die Wechseldatenträger wieder angeschlossen werden, wird die Verschlüsselungsrichtlinie korrekt angewendet.
- Auf einer stark fragmentierten Festplatte kann die Verschlüsselung möglicherweise nicht starten. Defragmentieren Sie die Festplatte.
- Wenn Festplatten verschlüsselt werden, wird der Ruhezustand ab dem Zeitpunkt des Beginns der Verschlüsselungsaufgabe bis zum ersten Neustart eines Computers mit Microsoft Windows 7/8/8.1/10 und nach der Installation der Festplattenverschlüsselung bis zum ersten Neustart von Microsoft Windows 8/8.1/10 Betriebssystemen blockiert. Wenn Festplatten entschlüsselt werden, wird der Ruhezustand ab dem Zeitpunkt, an dem das Startlaufwerk vollständig entschlüsselt ist, bis zum ersten Neustart des Betriebssystems blockiert. Wenn die **Schnellstart-Option** in Microsoft Windows 8/8.1/10 aktiviert ist, hindert die Blockierung des Ruhezustands Sie daran, das Betriebssystem herunterzufahren.
- Computer mit Windows 7 können das Kennwort während der Wiederherstellung nicht ändern, wenn das Laufwerk mit der BitLocker-Technologie verschlüsselt ist. Nachdem der Wiederherstellungsschlüssel eingegeben wurde und das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer nicht auf, das Kennwort oder den PIN-Code zu ändern. Daher ist es nicht möglich, ein neues Passwort oder einen neuen PIN-Code festzulegen. Dieses Problem beruht auf Besonderheiten des Betriebssystems. Um fortzufahren, müssen Sie die Festplatte neu verschlüsseln.
- Es wird nicht empfohlen, das Tool xbootmgr.exe mit aktivierten zusätzlichen Providern zu verwenden. Zum Beispiel Dispatcher, Netzwerk oder Treiber.
- Die Formatierung eines verschlüsselten Wechseldatenträgers wird auf einem Computer, auf dem Kaspersky Endpoint Security für Windows installiert ist, nicht unterstützt.
- Die Formatierung eines verschlüsselten Wechseldatenträgers mit dem FAT32-Dateisystem wird nicht unterstützt (das Laufwerk wird als verschlüsselt angezeigt). Um ein Laufwerk zu formatieren, formatieren Sie es in das NTFS-Dateisystem um.
- Einzelheiten zur Wiederherstellung eines Betriebssystems von einer Sicherungskopie auf ein verschlüsseltes GPT-Gerät finden Sie in der Wissensdatenbank des Technischen Supports.
- Mehrere Download-Agenten können nicht nebeneinander auf einem verschlüsselten Computer existieren.

- Es ist unmöglich, auf einen Wechseldatenträger zuzugreifen, der zuvor auf einem anderen Computer verschlüsselt wurde, wenn alle der folgenden Bedingungen gleichzeitig erfüllt sind:

  - Es besteht keine Verbindung zum Server des Kaspersky Security Center.
  - Der Benutzer versucht, sich mit einem neuen Token oder Kennwort zu autorisieren.

  Wenn eine ähnliche Situation eintritt, starten Sie den Computer neu. Nachdem der Computer neu gestartet wurde, wird der Zugriff auf den verschlüsselten Wechseldatenträger gewährt.

- Die Erkennung von USB-Geräten durch den Authentifizierungsagenten wird möglicherweise nicht unterstützt, wenn der xHCI-Modus für USB in den BIOS-Einstellungen aktiviert ist.

- Kaspersky Disk Encryption (FDE) für den SSD-Teil eines Geräts, der für die Zwischenspeicherung der am häufigsten verwendeten Daten verwendet wird, wird für SSHD-Geräte nicht unterstützt.

- Die Verschlüsselung von Festplatten in 32-Bit-Microsoft Windows 8/8.1/10-Betriebssystemen, die im UEFI-Modus laufen, wird nicht unterstützt.

- Starten Sie den Computer neu, bevor Sie eine entschlüsselte Festplatte erneut verschlüsseln.

- Die Festplattenverschlüsselung ist nicht kompatibel mit Kaspersky Anti-Virus für UEFI. Es wird nicht empfohlen, Festplattenverschlüsselung auf Computern zu verwenden, auf denen Kaspersky Anti-Virus für UEFI installiert ist.

- Das Erstellen von Authentifizierungsagent-Konten auf der Grundlage von Microsoft-Konten wird mit den folgenden Einschränkungen unterstützt:

  - Die Single-Sign-On-Technologie wird nicht unterstützt.
  - Die automatische Erstellung von Authentifizierungsagent-Konten wird nicht unterstützt, wenn die Option zur Erstellung von Konten für Benutzer, die sich in den letzten n Tagen am System angemeldet haben, ausgewählt wurde.

- Wenn der Name eines Authentifizierungsagent-Kontos im Format `<Domäne>/<Windows-Kontoname>` vorliegt, müssen Sie nach der Änderung des Computernamens auch die Namen von Konten ändern, die für lokale Benutzer dieses Computers erstellt wurden. Stellen Sie sich zum Beispiel vor, es gibt einen lokalen Benutzer `Ivanov` auf dem `Ivanov-Computer`, und für diesen Benutzer wurde ein Authentifizierungsagent-Konto mit dem Namen `Ivanov/Ivanov` erstellt. Wenn der Computername `Ivanov` in `Ivanov-PC` geändert wurde, müssen Sie den Namen des Authentifizierungsagent-Kontos für den Benutzer `Ivanov` von `Ivanov/Ivanov` in `Ivanov-PC/Ivanov` ändern. Sie können den Kontonamen ändern, indem Sie die Verwaltungsaufgabe für lokale Konten des Authentifizierungsagenten verwenden. Bevor der Name des Kontos geändert wurde, ist die Authentifizierung in der Pre-Boot-Umgebung mit dem alten Namen möglich (z. B. `Ivanov/Ivanov`).

- Wenn ein Benutzer nur mit einem Token auf einen Computer zugreifen darf, der mit der Kaspersky Disk Encryption-Technologie verschlüsselt wurde, und dieser Benutzer das Verfahren zur Wiederherstellung des Zugriffs abschließen muss, stellen Sie sicher, dass diesem Benutzer nach der Wiederherstellung des Zugriffs auf den verschlüsselten Computer kennwortbasierter Zugriff auf diesen Computer gewährt wird. Das Kennwort, das der Benutzer bei der Wiederherstellung des Zugriffs festgelegt hat, wird möglicherweise nicht gespeichert. In diesem Fall muss der Benutzer das Verfahren zur Wiederherstellung des Zugriffs auf den verschlüsselten Computer beim nächsten Neustart des Computers erneut durchführen.

- Beim Entschlüsseln einer Festplatte mit dem FDE Recovery Tool kann der Entschlüsselungsprozess mit einem Fehler enden, wenn Daten auf dem Quellgerät mit den entschlüsselten Daten überschrieben werden. Ein Teil der Daten auf der Festplatte bleibt verschlüsselt. Es wird empfohlen, die Option zum Speichern entschlüsselter Daten in eine Datei in den Geräteentschlüsselungseinstellungen zu wählen, wenn das FDE-Wiederherstellungs-Tool verwendet wird.

- Wenn das Kennwort des Authentifizierungsagenten geändert wurde, erscheint eine Nachricht mit dem Text *Ihr Kennwort wurde erfolgreich geändert. Klicken Sie auf OK* erscheint und der Benutzer startet den Computer neu. Das neue Kennwort wird nicht gespeichert. Das alte Kennwort muss für die nachfolgende Authentifizierung in der Pre-Boot-Umgebung verwendet werden.

- Die Festplattenverschlüsselung ist mit der Intel Rapid Start-Technologie inkompatibel.

- Die Festplattenverschlüsselung ist mit der ExpressCache-Technologie nicht kompatibel.

- In einigen Fällen erkennt das Tool beim Versuch, ein verschlüsseltes Laufwerk mit dem FDE Recovery Tool zu entschlüsseln, fälschlicherweise den Gerätestatus als „unverschlüsselt“, nachdem das „Anfrage-Antwort“-Verfahren abgeschlossen ist. Das Protokoll des Tools zeigt ein Ereignis, das besagt, dass das Gerät erfolgreich entschlüsselt wurde. In diesem Fall müssen Sie das Datenwiederherstellungsverfahren neu starten, um das Gerät zu entschlüsseln.

- Nachdem das Plug-In von Kaspersky Endpoint Security für Windows in der Web Console aktualisiert wurde, zeigen die Eigenschaften des Client-Computers den BitLocker-Wiederherstellungsschlüssel erst nach dem Neustart des Web Console-Dienstes an.

- Weitere Informationen zu den anderen Einschränkungen der Unterstützung der vollen Festplattenverschlüsselung und eine Liste der Geräte, für die die Festplattenverschlüsselung mit Einschränkungen unterstützt wird, finden Sie in der Wissensdatenbank des Technischen Supports.

Verschlüsselung von Dateien (File Level Encryption, FLE).

- Die Datei- und Ordnerverschlüsselung wird in Betriebssystemen der Microsoft Windows Embedded-Familie nicht unterstützt.
- Nachdem Sie die Anwendung installiert haben, müssen Sie das Betriebssystem neu starten, damit die Datei- und Ordnerverschlüsselung ordnungsgemäß funktioniert.
- Wenn eine verschlüsselte Datei auf einem Computer gespeichert ist, der über eine verfügbare Verschlüsselungsfunktion verfügt, und Sie auf die Datei von einem Computer zugreifen, auf dem keine Verschlüsselung verfügbar ist, wird ein direkter Zugriff auf diese Datei ermöglicht. Eine verschlüsselte Datei, die in einem Netzwerkordner auf einem Computer gespeichert ist, der über eine verfügbare Verschlüsselungsfunktion verfügt, wird in entschlüsselter Form auf einen Computer kopiert, der nicht über eine verfügbare Verschlüsselungsfunktion verfügt.
- Es wird empfohlen, Dateien zu entschlüsseln, die mit Encrypting File System verschlüsselt wurden, bevor Sie Dateien mit Kaspersky Endpoint Security für Windows verschlüsseln.
- Nachdem eine Datei verschlüsselt wurde, erhöht sich ihre Größe um 4 KB.
- Nachdem eine Datei verschlüsselt wurde, wird das Attribut *Archiv* in den Dateieigenschaften gesetzt.
- Wenn eine aus einem verschlüsselten Archiv entpackte Datei den gleichen Namen hat wie eine bereits auf Ihrem Computer vorhandene Datei, so wird letztere durch die neue, aus dem verschlüsselten Archiv entpackte Datei überschrieben. Der Benutzer wird nicht über den Überschreibvorgang benachrichtigt.
- Die Schnittstelle des portablen Dateimanagers zeigt keine Meldungen über Fehler an, die während seines Betriebs auftreten.
- Kaspersky Endpoint Security für Windows startet den portablen Dateimanager nicht auf einem Computer, auf dem die Komponente „Dateien verschlüsseln“ installiert ist.
- Der portable Dateimanager kann nicht für den Zugriff auf einen Wechseldatenträger verwendet werden, wenn die folgenden Bedingungen gleichzeitig zutreffen:
  - Es besteht keine Verbindung zu Kaspersky Security Center.
  - Kaspersky Endpoint Security für Windows ist auf dem Computer installiert.
  - Auf dem Computer ist keine Datenverschlüsselung (FDE oder FLE) erfolgt.

  In einem solchen Fall ist der Zugriff auch dann nicht möglich, wenn Ihnen das Kennwort für den portablen Dateimanager bekannt ist.
- Wenn die Dateiverschlüsselung verwendet wird, ist das Programm nicht mit dem Mail-Client Sylpheed kompatibel.
- Kaspersky Endpoint Security für Windows unterstützt die Regeln zur Zugriffsbeschränkung auf verschlüsselte Dateien für einige Apps nicht. Das liegt daran, dass einige Dateivorgänge durch Drittanbieter-Programme ausgeführt werden. Beispielsweise wird das Kopieren von Dateien durch den Dateimanager ausgeführt, nicht durch die App. Falls dem E-Mail-Client Outlook der Zugriff auf verschlüsselte Dateien verweigert wird, ermöglicht Kaspersky Endpoint Security dem E-Mail-Client auf diese Weise den Zugriff auf die verschlüsselte Datei, wenn der Benutzer Dateien über die Zwischenablage oder mit Drag-and-Drag-Funktion in die E-Mail-Nachricht kopiert hat. Der Kopiervorgang wurde von einem Dateimanager durchgeführt, für den keine Regeln zur Einschränkung des Zugriffs auf verschlüsselte Dateien festgelegt sind, d. h. der Zugriff ist erlaubt.

- Das Ändern der Seitendatei-Einstellungen wird nicht unterstützt. Das Betriebssystem verwendet die Standardwerte anstelle der angegebenen Parameterwerte.
- Verwenden Sie das sichere Entfernen, wenn Sie mit verschlüsselten Wechseldatenträgern arbeiten. Wir können die Datenintegrität nicht garantieren, wenn der Wechseldatenträger nicht sicher entfernt wird.
- Nachdem die Dateien verschlüsselt wurden, werden ihre unverschlüsselten Originale sicher gelöscht.
- Die Synchronisierung von Offline-Dateien mithilfe von Client-seitigem Caching (CSC) wird nicht unterstützt. Es wird empfohlen, die Offline-Verwaltung von gemeinsam genutzten Ressourcen auf der Ebene der Gruppenrichtlinien zu verbieten. Dateien, die sich im Offline-Modus befinden, können bearbeitet werden. Nach der Synchronisierung können an einer Offline-Datei vorgenommene Änderungen verloren gehen. Einzelheiten zur Unterstützung von Client-Side Caching (CSC) bei der Verwendung von Verschlüsselung finden Sie in der Wissensdatenbank des Technischen Supports.
- Die Erstellung eines verschlüsselten Archivs im Stammverzeichnis der Systemfestplatte wird nicht unterstützt.
- Beim Zugriff auf verschlüsselte Dateien über das Netzwerk können Probleme auftreten. Es wird empfohlen, die Dateien in eine andere Quelle zu verschieben oder sicherzustellen, dass der Computer, der als Dateiserver verwendet wird, vom gleichen Kaspersky Security Center-Administrationsserver verwaltet wird.
- Eine Änderung des Tastaturlayouts kann dazu führen, dass das Kennworteingabefenster für ein verschlüsseltes selbstextrahierendes Archiv hängen bleibt. Um dieses Problem zu beheben, schließen Sie das Kennworteingabefenster, ändern Sie das Tastaturlayout in Ihrem Betriebssystem und geben Sie das Kennwort für das verschlüsselte Archiv erneut ein.
- Wenn die Dateiverschlüsselung auf Systemen mit mehreren Partitionen auf einer Festplatte verwendet wird, empfiehlt es sich, die Option zu verwenden, die automatisch die Größe der pagefile.sys-Datei bestimmt. Nach dem Neustart des Computers kann sich die pagefile.sys-Datei zwischen den Festplattenpartitionen bewegen.
- Stellen Sie nach dem Anwenden der Dateiverschlüsselungsregeln, einschließlich der Dateien im Ordner „Eigene Dateien“, sicher, dass Benutzer, für die die Verschlüsselung angewendet wurde, erfolgreich auf verschlüsselte Dateien zugreifen können. Dazu muss sich jeder Benutzer beim System anmelden, wenn eine Verbindung zum Kaspersky Security Center verfügbar ist. Wenn ein Benutzer versucht, auf verschlüsselte Dateien zuzugreifen, ohne eine Verbindung zum Kaspersky Security Center zu haben, kann das System hängen.
- Wenn Systemdateien irgendwie in den Geltungsbereich der Verschlüsselung auf Dateiebene einbezogen sind, können Ereignisse bezüglich Fehlern beim Verschlüsseln dieser Dateien in Berichten erscheinen. Die in diesen Ereignissen angegebenen Dateien sind nicht wirklich verschlüsselt.
- Pico-Prozesse werden nicht unterstützt.
- Groß-/Kleinschreibung von Pfaden wird nicht unterstützt. Wenn Verschlüsselungsregeln oder Entschlüsselungsregeln angewendet werden, werden die Pfade in Produktereignissen in Kleinbuchstaben angezeigt.
- Es wird nicht empfohlen, Dateien zu verschlüsseln, die vom System beim Systemstart verwendet werden. Wenn diese Dateien verschlüsselt sind, kann der Versuch, auf verschlüsselte Dateien ohne Verbindung zum Kaspersky Security Center zuzugreifen, zum Hängen des Systems oder zu Aufforderungen zum Zugriff auf unverschlüsselte Dateien führen.
- Wenn Wechseldatenträger mit Unterstützung des portablen Modus verschlüsselt sind, kann die Kontrolle des Alters des Kennworts nicht deaktiviert werden.

- Wenn Benutzer gemeinsam mit einer Datei über das Netzwerk unter FLE-Regeln über Programme, die die Datei-zu-Speicher-Zuordnungsmethode verwenden (wie WordPad oder FAR), und Programme, die für die Arbeit mit großen Dateien ausgelegt sind (wie Notepad ++), arbeiten, kann die Datei in unverschlüsselter Form auf unbestimmte Zeit blockiert werden, ohne die Möglichkeit, von dem Computer, auf dem sie sich befindet, darauf zuzugreifen.

- Dateiverschlüsselung in OneDrive-Synchronisationsordnern wird nicht unterstützt. Das Hinzufügen von Ordnern mit bereits verschlüsselten Dateien zur OneDrive-Synchronisationsliste kann zu Datenverlusten in den verschlüsselten Dateien führen.

- Wenn die Verschlüsselungskomponente auf Dateiebene installiert ist, funktioniert die Verwaltung von Benutzern und Gruppen nicht im WSL-Modus (Windows-Subsystem für Linux).

- Wenn die Verschlüsselungskomponente auf Dateiebene installiert ist, wird POSIX (Portable Operating System Interface) zum Umbenennen und Löschen von Dateien nicht unterstützt.

- Stellen Sie nach dem Update von Kaspersky Endpoint Security für Windows Version 11.0.1 oder früher sicher, dass der Administrationsagent ausgeführt wird, um nach dem Neustart des Computers auf verschlüsselte Dateien zugreifen zu können. Der Administrationsagent hat einen verzögerten Start, sodass Sie nicht sofort nach dem Laden des Betriebssystems auf die verschlüsselten Dateien zugreifen können. Sie müssen nicht warten, bis der Administrationsagent nach dem nächsten Computerstart gestartet wird.

Andere Einschränkungen

- In Serverbetriebssystemen wird keine Warnung bezüglich der Notwendigkeit einer erweiterten Desinfektion angezeigt.
- Webadressen, die der Liste der vertrauenswürdigen Adressen hinzugefügt werden, werden möglicherweise nicht korrekt verarbeitet.
- Kaspersky Endpoint Security überwacht den HTTP-Datenverkehr, der den Standards RFC 2616, RFC 7540, RFC 7541 und RFC 7301 entspricht. Wenn Kaspersky Endpoint Security ein anderes Übertragungsformat im HTTP-Datenverkehr erkennt, sperrt die Anwendung diese Verbindung, um einen Download von bösartigem Code aus dem Internet zu verhindern.
- Kaspersky Endpoint Security unterstützt den Standard RFC9218 für das HTTP/2-Protokoll nicht. Wenn Kaspersky Endpoint Security dieses Übertragungsformat im Datenverkehr erkennt, sperrt das Programm diese Verbindung und im Browser wird der Fehler ERR_HTTP2_PROTOCOL_ERROR angezeigt. Wenn Sie die betreffende Webressource benötigen, können Sie die Webressource von der Untersuchung verschlüsselter Verbindungen ausschließen oder beim Technischen Support einen Patch anfordern.
- Aktivitätsmonitor. Vollständige Informationen über Prozesse werden nicht angezeigt.
- Wenn Kaspersky Endpoint Security für Windows zum ersten Mal gestartet wird, kann es vorkommen, dass ein digital signiertes Programm vorübergehend in die falsche Gruppe verschoben wird. Der digital signierte Antrag wird später in die richtige Gruppe gestellt.
- Wenn Sie E-Mails mit der Schutz vor E-Mail-Bedrohungen-Erweiterung für Microsoft Outlook untersuchen, wird empfohlen, den Cached Exchange-Modus zu verwenden (die Option Cached Exchange-Modus verwenden).
- Die Aufgabe *Untersuchung auf Viren* unterstützt die 64-Bit-Version von Microsoft Outlook nicht. Das bedeutet, dass Kaspersky Endpoint Security die Dateien des Typs Outlook x64 (PST- und OST-Dateien) nicht untersucht, und zwar auch dann nicht, wenn eine E-Mail-Nachricht zum Untersuchungsbereich gehört.
- In Kaspersky Security Center 10 wird beim Wechsel von der Verwendung des globalen Kaspersky Security Network zur Verwendung eines privaten Kaspersky Security Network oder umgekehrt die Option zur Teilnahme am Kaspersky Security Network in der Richtlinie des entsprechenden Produkts deaktiviert. Lesen Sie nach dem Wechsel den Text der Erklärung zum Kaspersky Security Network sorgfältig durch und bestätigen Sie Ihr Einverständnis zur Teilnahme am KSN. Sie können den Text der Erklärung in der Programmoberfläche oder beim Bearbeiten der Produktrichtlinie lesen.
- Bei einer erneuten Untersuchung eines bösartigen Objekts, das durch Software von Drittanbietern blockiert wurde, wird der Benutzer nicht benachrichtigt, wenn die Bedrohung erneut erkannt wird. Das Ereignis der erneuten Erkennung der Bedrohung wird im Produktbericht und im Bericht des Kaspersky Security Center 10 angezeigt.
- Die Komponente Endpunktsensor kann nicht in Microsoft Windows Server 2008 installiert werden.
- Der Bericht von Kaspersky Security Center 10 zur Geräteverschlüsselung enthält keine Informationen über Geräte, die mit Microsoft BitLocker auf Serverplattformen oder auf Arbeitsstationen verschlüsselt wurden, auf denen die Komponente Device Control nicht installiert ist.
- Bei Verwendung einer Richtlinienhierarchie sind die Einstellungen des Abschnitts „Verschlüsselung von Wechseldatenträgern“ in einer untergeordneten Richtlinie zur Bearbeitung zugänglich, wenn die übergeordnete Richtlinie die Änderung dieser Einstellungen verbietet.
- Sie müssen die Anmeldungsüberwachung in den Betriebssystemeinstellungen aktivieren, um das ordnungsgemäße Funktionieren der Ausnahmen für den Schutz von freigegebenen Ordnern vor externer

Verschlüsselung zu gewährleisten.

- Wenn der Schutz gemeinsamer Ordner aktiviert ist, versucht Kaspersky Endpoint Security für Windows, gemeinsame Ordner für jede Remote-Zugriffssitzung zu verschlüsseln, die vor dem Start von Kaspersky Endpoint Security für Windows gestartet wurde, auch wenn der Computer, von dem die Remote-Zugriffssitzung gestartet wurde, zu den Ausnahmen hinzugefügt wurde. Wenn Sie nicht möchten, dass Kaspersky Endpoint Security für Windows Versuche zur Verschlüsselung von freigegebenen Ordnern für Remote-Zugriffssitzungen überwacht, die von einem Computer gestartet wurden, der zu den Ausnahmen hinzugefügt wurde und der vor dem Start von Kaspersky Endpoint Security für Windows gestartet wurde, beenden Sie die Remote-Zugriffssitzung und bauen Sie sie wieder auf oder starten Sie den Computer neu, auf dem Kaspersky Endpoint Security für Windows installiert ist.

- Wenn die Aktualisierungsaufgabe mit den Berechtigungen eines bestimmten Benutzerkontos ausgeführt wird, werden Produkt-Patches nicht heruntergeladen, sofern die Aktualisierung von einer Quelle erfolgt, die eine Autorisierung erfordert.

- Der Start des Programms kann aufgrund unzureichender Systemleistung fehlschlagen. Um dieses Problem zu beheben, verwenden Sie die Option „Bereit zum Booten“ oder erhöhen Sie die Zeitüberschreitung des Betriebssystems zum Starten von Diensten.

- Das Programm kann nicht im abgesicherten Modus arbeiten.

- Um sicherzustellen, dass Kaspersky Endpoint Security für Windows Versionen 11.5.0 und 11.6.0 ordnungsgemäß mit Cisco AnyConnect-Software funktioniert, müssen Sie die Kompatibilitätsmodul-Version 4.3.183.2048 oder höher installieren. Mehr über die Kompatibilität mit der Cisco Identity Services Engine erfahren Sie in der Cisco-Dokumentation.

- Wir können nicht garantieren, dass die Audiosteuerung beim ersten Neustart nach der Installation des Programms funktioniert.

- Wenn rotierende Ablaufverfolgungsdateien aktiviert sind, werden keine Ablaufverfolgungen für die AMSI-Komponente und das Outlook-Plug-in erstellt.

- Leistungsspuren können in Windows Server 2008 nicht manuell erfasst werden.

- Leistungsspuren für den Spurentyp „Neustart“ werden nicht unterstützt.

- Die KSN-Verfügbarkeitsprüfung wird nicht mehr unterstützt.

- Wenn Sie die Option „Externe Verwaltung der Systemdienste deaktivieren“ ausschalten, können Sie den Dienst des Programms, das mit dem Parameter `AMPPL=1` installiert wurde, nicht stoppen (standardmäßig ist der Parameterwert ab der Betriebssystemversion Windows 10RS2 auf `1` gesetzt). Der Parameter `AMPPL` mit einem Wert von `1` ermöglicht die Verwendung der Schutzprozess-Technologie für den Produktservice.

- Um eine benutzerdefinierte Untersuchung eines Ordners auszuführen, muss der Benutzer, der die benutzerdefinierte Untersuchung startet, über die Berechtigungen zum Lesen der Attribute dieses Ordners verfügen. Andernfalls ist die Untersuchung des benutzerdefinierten Ordners nicht möglich und endet mit einem Fehler.

- Wenn eine in einer Richtlinie definierte Untersuchungsregel einen Pfad ohne das Zeichen `\` am Ende enthält, z. B. `C:\ordner1\ordner2`, wird die Untersuchung für den Pfad C:\ordner1\ ausgeführt.

- Bei einem Upgrade des Programms von Version 11.1.0 auf 11.6.0 werden die „AMSI-Schutz“-Einstellungen auf ihre Standardwerte zurückgesetzt.

- Wenn Sie Richtlinien für Softwareeinschränkung (Software Restriction Policies, SRP) verwenden, kann der Computer möglicherweise nicht starten (schwarzer Bildschirm). Es wird empfohlen, die SRP-Einstellungen

wie folgt zu ändern: Setzen Sie den Wert **Alle Softwaredateien außer Bibliotheken (z. B. DLLs)** für den Parameter **Richtlinien für Softwareeinschränkung anwenden auf** und fügen Sie Regeln mit der Sicherheitsstufe **Uneingeschränkt** für die Pfade der Programmdateien hinzu (`C:\Program Files\Common Files\Kaspersky Lab` und `C:\Program Files\Kaspersky Lab`). Details zur Verwendung von SRP finden Sie in der *Microsoft-Dokumentation*.

- Die Verwaltung von Outlook-Plug-in-Einstellungen über Rest API wird nicht unterstützt.
- Aufgabenablaufeinstellungen für einen bestimmten Benutzer können nicht über eine Konfigurationsdatei zwischen Geräten übertragen werden. Nachdem die Einstellungen aus einer Konfigurationsdatei übernommen wurden, geben Sie den Benutzernamen und das Kennwort manuell an.
- Nach der Installation eines Updates funktioniert die Aufgabe der Integritätsprüfung erst, wenn das System neu gestartet wird, um das Update anzuwenden.
- Wenn die rotierende Ablaufverfolgungsebene über das Ferndiagnoseprogramm geändert wird, zeigt Kaspersky Endpoint Security für Windows fälschlicherweise einen leeren Wert für die Ablaufverfolgungsebene an. Ablaufverfolgungsdateien werden jedoch entsprechend der korrekten Ablaufverfolgungsebene geschrieben. Wenn die rotierende Ablaufverfolgungsebene über die lokale Schnittstelle des Programms geändert wird, wird die Ablaufverfolgungsebene korrekt geändert, aber das Ferndiagnose-Dienstprogramm zeigt fälschlicherweise die Ablaufverfolgungsebene an, die zuletzt vom Dienstprogramm definiert wurde. Dies kann dazu führen, dass der Administrator nicht über aktuelle Informationen über die aktuelle Ablaufverfolgungsebene verfügt und dass relevante Informationen in den Protokollen fehlen, wenn ein Benutzer die Ablaufverfolgungsebene manuell in der lokalen Oberfläche des Programms ändert.
- Auf der lokalen Benutzeroberfläche verhindern die Kennwortschutz-Einstellungen das Ändern des Administratorkontos (Standardwert: KLAdmin). Um den Namen des Administratorkontos zu ändern, müssen Sie den Kennwortschutz deaktivieren, dann den Kennwortschutz aktivieren und einen neuen Namen für das Administratorkonto angeben.
- Kaspersky Endpoint Security überwacht den HTTP-Datenverkehr, der den Standards RFC 2616, RFC 7540, RFC 7541 und RFC 7301 entspricht. Wenn Kaspersky Endpoint Security ein anderes Übertragungsformat im HTTP-Datenverkehr erkennt, sperrt die Anwendung diese Verbindung, um einen Download von bösartigem Code aus dem Internet zu verhindern.
- Wenn eine verschlüsselte Verbindung untersucht wird, erzwingt Kaspersky Endpoint Security das HTTP/1.
- Wenn Kaspersky Endpoint Security auf einem Server mit Windows Server 2019 installiert ist, ist die Anwendung inkompatibel mit Docker. Die Bereitstellung von Docker-Containern auf einem Computer mit Kaspersky Endpoint Security führt zu einem Absturz (BSOD).

Glossar

Administrationsagent

Programmkomponente von Kaspersky Security Center, welche für die Interaktion zwischen dem Administrationsserver und den Kaspersky-Programmen verantwortlich ist, die auf einem konkreten Netzwerkknoten (Workstation oder Server) installiert sind. Die vorliegende Komponente ist einheitlich für alle Programme von Kaspersky, die unter dem Betriebssystem Windows laufen. Für die Programme, die unter anderen Betriebssystemen laufen, sind spezielle Versionen des Administrationsagenten vorgesehen.

Administrationsgruppe

Eine Reihe von Geräten, die anhand der auszuführenden Funktionen und der auf ihnen installierten Kaspersky-Programme zusammengefasst wurden. Die Gruppierung dient zur vereinfachten Verwaltung der Geräte als geschlossene Einheit. Zu einer Gruppe können weitere Gruppen gehören. Für jede in der Gruppe installierte Anwendung können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Aktiver Schlüssel

Schlüssel, der momentan für das Programm verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky im Moment der Veröffentlichung der Antiviren-Datenbanken bekannt sind. Die Einträge der Antiviren-Datenbanken ermöglichen es, bösartigen Code in untersuchten Objekten zu finden. Die Antiviren-Datenbanken werden von den Kaspersky-Spezialisten gepflegt und stündlich aktualisiert.

Archiv

Eine oder mehrere Dateien, die in komprimierter Form in eine Datei aufgenommen wurden. Für die Archivierung und zum Entpacken von Daten ist ein spezielles Archivierungsprogramm erforderlich.

Aufgabe

Funktionen, die das Programm Kaspersky ausführt und die als Aufgaben konzipiert sind, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Untersuchung des Geräts, Datenbanken-Update.

Authentifizierungsagent

Schnittstelle, welche nach der Verschlüsselung einer bootfähigen Festplatte die Authentifizierung für den Zugriff auf verschlüsselte Festplatten und für das Laden des Betriebssystems ermöglicht.

Datenbank für bösartige Webadressen

Eine Liste der Webressourcen, deren Inhalt als gefährlich eingestuft werden kann. Die Liste wird von Kaspersky-Spezialisten erstellt. Sie wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Programms.

Datenbank für Phishing-Webadressen

Eine Liste der Webressourcen, die von den Spezialisten von Kaspersky als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Programms.

Desinfektion von Objekten

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

Fehlalarm

Situation, in der eine virenfreie Datei von der Kaspersky-Anwendung als infiziert eingestuft wird, da ihr Code Ähnlichkeit mit einem Virus aufweist.

Infizierte Datei

Datei, die schädlichen Code enthält (bei der Untersuchung der Datei wurde der Code eines bekannten bedrohlichen Programms gefunden). Die Kaspersky-Spezialisten warnen davor, mit solchen Dateien zu arbeiten, da dies zur Infektion Ihres Computers führen kann.

Lizenzzertifikat

Dokument, das Sie zusammen mit einer Schlüsseldatei oder einem Aktivierungscode von Kaspersky erhalten. Dieses Dokument enthält Informationen über die Lizenz, die Ihnen zur Verfügung gestellt wird.

Maske

Aus allgemeinen Zeichen bestehender Platzhalter für Dateinamen und -erweiterungen.

Zum Erstellen einer Dateimaske können alle für Dateinamen zulässigen Symbole einschließlich folgender Sonderzeichen verwendet werden:

- Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auch leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.

- Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamen eine beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung txt im Ordner `Folder` und in den Unterordnern. Die Maske muss mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht. Die Maske ** ist nur für die Erstellung von Untersuchungsausnahmen verfügbar.

- Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TXT haben und deren Name aus drei Zeichen besteht.

Normalisierte Form der Adresse einer Webressource

Als normalisierte Form der Adresse einer Webressource gilt die Textdarstellung der Adresse einer Webressource, die durch eine Normalisierung erreicht wird. Bei der Normalisierung wird die Textdarstellung einer Webadresse nach bestimmten Regeln verändert (z. B. Ausschluss von Benutzername, Kennwort und Verbindungsport aus der Textdarstellung der Webadresse, Umwandlung von in der Webadresse vorkommenden Großbuchstaben in Kleinbuchstaben).

Im Kontext der Schutzkomponenten besteht das Ziel einer Normalisierung der Adressen von Webressourcen darin, syntaktisch unterschiedliche, physisch jedoch äquivalente Adressen von Webadressen nur einmal zu untersuchen.

Beispiel:

Nicht normalisierte Form einer Adresse: www.Example.com\.

Normalisierte Form einer Adresse: www.example.com.

OLE-Objekt

Datei, die an eine andere Datei angehängt oder darin eingebettet ist. Die Programme von Kaspersky gestatten es, OLE-Objekte auf Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel® in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

Portabler Dateimanager

Programm, das eine Schnittstelle für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern bietet, wenn die Verschlüsselungsfunktionalität auf einem Computer nicht verfügbar ist.

Potenziell infizierbare Datei

Datei, die aufgrund ihrer Struktur oder ihres Formats von einem Angreifer als „Container“ benutzt werden kann, um Schadcode zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Für solche Dateien ist das Risiko, dass bösartiger Code eindringt, relativ hoch.

Schutzbereich

Objekte, die permanent von der Komponente für den Basisschutz untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften.

Trusted Platform Module

Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten.

Untersuchungsbereich

Objekte, die im Rahmen einer Untersuchungsaufgabe von Kaspersky Endpoint Security untersucht werden.

Zertifikataussteller

Zertifizierungsstelle, die das Zertifikat ausgestellt hat

Zusätzlicher Schlüssel

Dieser Schlüssel gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet.

Anhänge

Die Informationen in diesem Abschnitt ergänzen den allgemeinen Text des Dokuments.

Anhang 1. Programmeinstellungen

Sie können eine Richtlinie, Aufgaben oder die Programmoberfläche verwenden, um Kaspersky Endpoint Security zu konfigurieren. Ausführliche Informationen über die Programmkomponenten finden Sie in den entsprechenden Unterabschnitten.

Schutz vor bedrohlichen Dateien

Die Komponente „Schutz vor bedrohlichen Dateien“ schützt das Dateisystem des Computers vor einer Infektion. Die Komponente „Schutz vor bedrohlichen Dateien“ befindet sich standardmäßig permanent im Arbeitsspeicher des Computers. Die Komponente untersucht die Dateien auf allen Laufwerken des Computers sowie auf verbundenen Datenträgern. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Die Komponente untersucht die Dateien, auf die der Benutzer oder ein Programm zugreift. Beim Fund einer schädlichen Datei blockiert Kaspersky Endpoint Security den Vorgang mit dieser Datei. Das Programm desinfiziert oder löscht die schädliche Datei. Das Vorgehen ist von den Einstellungen der Komponente „Schutz vor bedrohlichen Dateien“ abhängig.

Beim Zugriff auf eine Datei, deren Inhalt sich im Cloud-Speicher OneDrive befindet, lädt Kaspersky Endpoint Security den Inhalt dieser Datei herunter und untersucht ihn.

Einstellungen der Komponente „Schutz vor bedrohlichen Dateien”

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Zum Schutz vor bedrohlichen Dateien kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser Sicherheitsstufe für Dateien kontrolliert die Komponente „Schutz vor bedrohlichen Dateien“ alle Dateien, die geöffnet, gespeichert und gestartet werden, mit höchster Genauigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht alle Dateitypen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Untersucht werden außerdem Archive, Installationspakete und eingebettete OLE-Objekte. • **Empfohlen**. Diese Sicherheitsstufe für Dateien wird von Kaspersky-Experten empfohlen. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht Archive oder Installationspakete nicht. • **Niedrig**. Diese Sicherheitsstufe für Dateien bietet eine maximale Untersuchungsgeschwindigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers.

	Zusammengesetzte Dateien werden von der Komponente „Schutz vor bedrohlichen Dateien“ nicht untersucht.
Dateitypen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	**Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Dateien nach Format untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht. **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.
Schutzbereich	Enthält die Objekte, die von der Komponente „Schutz vor bedrohlichen Dateien“ untersucht werden. Ein Untersuchungsobjekt kann sein: Festplatte, Wechseldatenträger oder Netzwerklaufwerk, Ordner, eine Datei oder mehrere Dateien, die durch eine Maske angegeben sind. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht standardmäßig die Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden. Der Schutzbereich dieser Objekte kann nicht geändert oder gelöscht werden. Es ist nur möglich, ein Objekt (z. B. Wechseldatenträger) von der Untersuchung auszuschließen.
Maschinelles Lernen und Signaturanalyse *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Aktion beim Fund einer Bedrohung	**Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.

	Blockieren Wenn diese Variante ausgewählt ist, blockiert die Komponente „Schutz vor bedrohlichen Dateien“ die infizierten Dateien automatisch, ohne einen Desinfektionsversuch zu unternehmen. Bevor Sie versuchen, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt Kaspersky Endpoint Security eine Sicherungskopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.
Nur neue und veränderte Dateien untersuchen	Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.
Archive untersuchen	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.
Programmpakete untersuchen	Dieses Kontrollkästchen aktiviert / deaktiviert die Untersuchung der Programmpakete von Drittherstellern.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Große zusammengesetzte Dateien nicht entpacken	Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe. Unabhängig vom Status dieses Kontrollkästchens untersucht Kaspersky Endpoint Security große Dateien, die aus Archiven extrahiert werden.
Zusammengesetzte Dateien im Hintergrund entpacken	Wenn das Kontrollkästchen aktiviert ist, gewährt Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, die größer sind als der festgelegte Wert. Der Zugriff wird gewährt, bevor diese Dateien untersucht werden. Dabei entpackt und untersucht Kaspersky Endpoint Security die zusammengesetzten Dateien im Hintergrundmodus. Kaspersky Endpoint Security gewährt den Zugriff auf zusammengesetzte Dateien, die kleiner sind als der festgelegte Wert. Der Zugriff wird erst gewährt, nachdem diese Dateien entpackt und untersucht wurden. Wenn das Kontrollkästchen deaktiviert ist, gewährt Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, erst nachdem die Dateien beliebiger Größe entpackt und untersucht wurden.
Untersuchungsmodus *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Kaspersky Endpoint Security untersucht Dateien, auf die der Benutzer, das Betriebssystem oder ein Programm, das unter dem Benutzerkonto des Benutzers läuft, zugreift.

	Intelligent. In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien“-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen. **Bei Zugriff und Veränderungen**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ Objekte jedes Mal untersucht, wenn versucht wird, diese zu öffnen oder zu bearbeiten. **Bei Zugriff**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu öffnen. **Bei Ausführung**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu starten.
iSwift-Technologie *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Schutz vor bedrohlichen Dateien anhalten *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Diese Option hält die Ausführung der Funktion „Schutz vor bedrohlichen Dateien“ zu den angegebenen Zeiten oder beim Start der angegebenen Programme vorübergehend automatisch an.

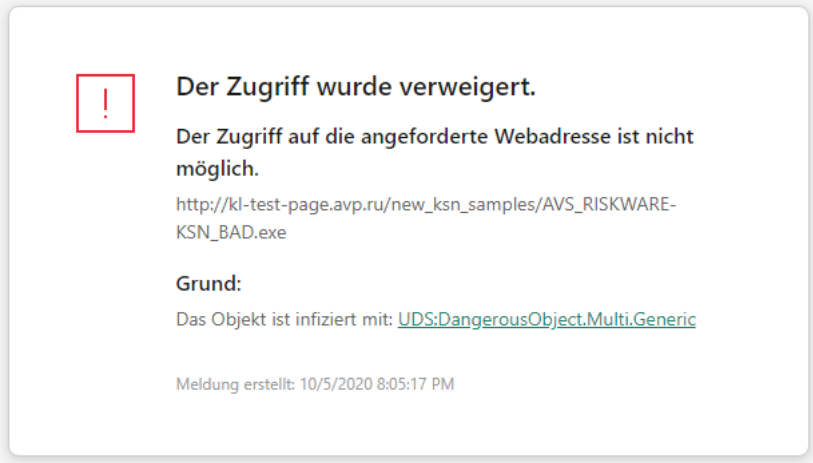
Schutz vor Web-Bedrohungen

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert schädliche Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Kaspersky Endpoint Security untersucht den HTTP-, HTTPS- und FTP-Datenverkehr. Kaspersky Endpoint Security untersucht URL- und IP-Adressen. Sie können die Ports angeben, die Kaspersky Endpoint Security kontrollieren soll, oder alle Ports auswählen.

Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

Wenn ein Benutzer versucht, eine schädliche Website oder eine Phishing-Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).



Benachrichtigung über ein Verbot des Zugriffs auf die Website

Einstellungen der Komponente „Schutz vor Web-Bedrohungen"

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Zum Schutz vor Web-Bedrohungen kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser Sicherheitsstufe für den Web-Datenverkehr untersucht die Komponente „Schutz vor Web-Bedrohungen" den Web-Datenverkehr, der über die Protokolle HTTP und FTP empfangen wird, mit höchster Genauigkeit. Der Schutz vor Web-Bedrohungen untersucht alle Objekte des Web-Datenverkehrs ausführlich, verwendet die vollständigen Programm-Datenbanken und führt zusätzlich eine heuristische Analyse mit maximaler Tiefe aus. • **Empfohlen**. Diese Sicherheitsstufe für den Web-Datenverkehr bietet ein optimales Verhältnis zwischen der Leistung von Kaspersky Endpoint Security und der Sicherheit für den Web-Datenverkehr. Die Komponente „Schutz vor Web-Bedrohungen" führt die heuristische Analyse auf der Stufe **Mittel** aus. Diese Sicherheitsstufe für den Web-Datenverkehr wird von den Kaspersky-Experten empfohlen. • **Niedrig**. Diese Sicherheitsstufe für den Web-Datenverkehr gewährleistet maximale Geschwindigkeit bei der Untersuchung des Web-Datenverkehrs. Die Komponente „Schutz vor Web-Bedrohungen" führt die heuristische Analyse auf der Stufe **Oberflächlich** aus.
Aktion beim Fund einer Bedrohung	**Download verbieten**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen" den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

	Informieren Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.
URL mit der Datenbank für bösartige URLs untersuchen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Heuristische Analyse verwenden *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Webadresse mit der Datenbank für Phishing-Webadressen untersuchen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen	Ist das Kontrollkästchen aktiviert, so untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Inhalt von Webseiten/Websites nicht, deren Adressen auf der Liste der vertrauenswürdigen Webadressen stehen. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website.

Schutz vor E-Mail-Bedrohungen

Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. Außerdem überprüft die Komponente, ob Nachrichten bösartige Links oder Phishing-Links enthalten. Die Komponente „Schutz vor E-Mail-Bedrohungen“ befindet sich standardmäßig permanent im Arbeitsspeicher des Computers und untersucht alle Nachrichten, die mit den Protokollen POP3, SMTP, IMAP und NNTP oder im Mail-Client Microsoft Office Outlook (MAPI) empfangen oder gesendet werden. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Wenn ein Mail-Client in einem Browser geöffnet ist, untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht.

Wenn in einer Anlage eine infizierte Datei gefunden wird, ändert Kaspersky Endpoint Security den Nachrichtenbetreff wie folgt: `[Nachricht ist infiziert] <Betreff der Nachricht>` oder `[Infiziertes Objekt wurde gelöscht] <Betreff der Nachricht>`.

Diese Komponente interagiert mit den Mail-Clients, die auf dem Computer installiert sind. Für den Mail-Client Microsoft Office Outlook gibt es eine Erweiterung mit zusätzlichen Einstellungen. Die Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Zum Schutz vor E-Mail-Bedrohungen kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser E-Mail-Sicherheitsstufe kontrolliert die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten mit höchster Genauigkeit. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mails und führt eine tiefe heuristische Analyse durch. Die E-Mail-Sicherheitsstufe **Hoch** wird für Umgebungen mit hohem Risiko empfohlen. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk ohne zentralisierten E-Mail-Schutz erfolgt. • **Empfohlen**. Diese E-Mail-Sicherheitsstufe bietet ein optimales Verhältnis zwischen der Leistung von Kaspersky Endpoint Security und der Sicherheit für E-Mails. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mail-Nachrichten und führt eine heuristische Analyse mit mittlerer Tiefe aus. Diese E-Mail-Sicherheitsstufe wird von den Kaspersky-Experten empfohlen. • **Niedrig**. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ nur eingehende E-Mail-Nachrichten, führt eine oberflächliche heuristische Analyse aus und scannt die an Nachrichten angehängten Archive nicht. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ E-Mail-Nachrichten mit maximaler Geschwindigkeit und beansprucht die Betriebssystemressourcen minimal. Die E-Mail-Sicherheitsstufe **Niedrig** wird für die Arbeit in einer gut geschützten Umgebung empfohlen. Ein Beispiel für eine solche Umgebung ist ein LAN eines Unternehmens mit zentralisiertem E-Mail-Schutz.
Aktion beim Fund einer	**Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Wird in einer

Bedrohung	eingehenden oder ausgehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Konnte das Objekt nicht desinfiziert werden, so löscht Kaspersky Endpoint Security das infizierte Objekt. Kaspersky Endpoint Security fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu: `[Ein infiziertes Objekt wurde gelöscht.] <Nachrichtenbetreff>`. **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, versieht Kaspersky Endpoint Security den Nachrichtenbetreff mit einer Warnung: `[Message infected] <Nachrichtenbetreff>`. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, so versucht Kaspersky Endpoint Security, das gefundene Objekt zu desinfizieren. Konnte das Objekt nicht desinfiziert werden, so blockiert Kaspersky Endpoint Security das Senden der Nachricht. Der Mail-Client zeigt einen Fehler an. **Blockieren** Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, so fügt Kaspersky Endpoint Security eine Warnung zum Nachrichtenbetreff hinzu: `[Die Nachricht ist infiziert.] <Nachrichtenbetreff>`. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, so blockiert Kaspersky Endpoint Security das Senden der Nachricht. Der Mail-Client zeigt einen Fehler an.
Schutzbereich *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Der *Schutzbereich* umfasst Objekte, welche während der Ausführung der Komponente untersucht werden: **Eingehende und ausgehende Nachrichten** oder **Nur eingehende Nachrichten**. Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.
POP3/SMTP/NNTP/IMAP-Datenverkehr untersuchen	Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung des E-Mail-Datenverkehrs, der mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen wird. Die Untersuchung wird von der Komponente "Schutz vor E-Mail-Bedrohungen" ausgeführt.
Erweiterung für Microsoft Outlook verbinden	Wenn das Kontrollkästchen aktiviert ist, ist die Untersuchung von E-Mail-Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, aktiviert. Die Untersuchung erfolgt durch die in Microsoft Outlook integrierte Erweiterung. Erfolgt die E-Mail-Untersuchung mithilfe der Erweiterung für Microsoft Outlook, so wird empfohlen, den Exchange-Cache-Modus zu verwenden (Use Cached Exchange Mode). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.
Heuristische Analyse	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.

(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)	Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Angehängte Archive untersuchen	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE. Falls Kaspersky Endpoint Security während der Untersuchung im Text der Nachricht ein Kennwort für ein Archiv erkennt, wird dieses Kennwort verwendet, um den Inhalt des Archivs auf bösartige Anwendungen zu untersuchen. Das Kennwort wird in diesem Fall nicht gespeichert. Ein Archiv wird während der Untersuchung entpackt. Wenn während des Entpackungsvorgangs ein Anwendungsfehler auftritt, können Sie die unter dem folgenden Pfad gespeicherten entpackten Dateien manuell löschen: %systemroot%\temp. Diese Dateien besitzen das Präfix PR.
Angehängte Office-Format-Dateien untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Archive nicht untersuchen, wenn größer als ... MB	Ist das Kontrollkästchen aktiviert, so schließt die Komponente „Schutz vor E-Mail-Bedrohungen“ die Archive, die an E-Mail-Nachrichten angehängt sind, von der Untersuchung aus, falls sie die festgelegte Größe überschreiten. Ist das Kontrollkästchen deaktiviert, so untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die an E-Mail-Nachrichten angehängten Archive unabhängig von deren Größe.
Archive untersuchen für höchstens n Sek.	Wenn dieses Kontrollkästchen aktiviert ist, wird die Untersuchungsdauer für Archive, die an E-Mail-Nachrichten angehängt sind, auf die festgelegte Dauer beschränkt.
Anlagenfilterung	Die Anlagenfilterung funktioniert nicht für ausgehende E-Mail-Nachrichten. **Filterung deaktivieren**. Bei Auswahl dieser Variante werden Dateien, die an E-Mail-Nachrichten angehängt sind, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht gefiltert. **Anlagen der ausgewählten Typen umbenennen**. Wenn Sie diese Option auswählen, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Erweiterung angehängter Dateien bestimmter Typen mit einem Unterstrich (z. B. attachment.doc_). Der Benutzer muss die Datei dann zunächst umbenennen, um sie öffnen zu können. **Anlagen der ausgewählten Typen löschen**. Bei Auswahl dieser Variante löscht die Komponente „Schutz vor E-Mail-Bedrohungen“ aus E-Mail-Nachrichten die angehängten Dateien der angegebenen Typen. Die Typen der angehängten Dateien, die umbenannt und aus E-Mail-Nachrichten gelöscht werden sollen, können Sie in der Liste der Dateimasken festlegen.

Schutz vor Netzwerkbedrohungen

Die Komponente „Schutz vor Netzwerkbedrohungen“ (IDS, Intrusion Detection System) überwacht den eingehenden Netzwerkverkehr auf Aktivität, die für Netzwerkangriffe typisch ist. Wenn Kaspersky Endpoint Security einen Netzwerkangriff auf den Computer erkennt, sperrt das Programm die Netzwerkverbindung mit dem angreifenden Computer.

Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Die Liste der Netzwerkangriffe, die von der Komponente „Schutz vor Netzwerkbedrohungen“ erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Einstellungen für die Komponente „Schutz vor Netzwerkbedrohungen“

Einstellung	Beschreibung
Portscannen und Netzwerk-Flooding-Angriffe erkennen	*Network Flooding* ist ein Angriff auf die Netzwerkressourcen einer Organisation (z. B. auf einen Webserver). Bei diesem Angriff wird eine große Anzahl von Anforderungen gesendet, was die Bandbreite der Netzwerkressourcen überlastet. In einem solchen Fall können Benutzer nicht auf die Netzwerkressourcen der Organisation zugreifen. Beim Angriff *Port Scanning* werden die UDP-Ports, TCP-Ports und Netzwerkdienste des Computers gescannt. Bei diesem Angriff können Angreifer ermitteln, wie anfällig der Computer für Angriffe ist, bevor sie gefährlichere Arten von Netzwerkangriffen starten. Mithilfe von Port Scanning können Angreifer außerdem das Betriebssystem des Computers identifizieren und die entsprechenden Netzwerkangriffe für dieses Betriebssystem auswählen. Wenn dieses Kontrollkästchen aktiviert ist, überwacht Kaspersky Endpoint Security den Netzwerkverkehr, um diese Angriffe zu erkennen. Wenn ein Angriff erkannt wird, filtert und blockiert das Programm den mit dem Angriff verbundenen Datenverkehr. Auf diese Weise reduziert das Programm die Auslastung der angegriffenen Ressource, wenn ein Network-Flooding-Angriff auf den Computer gestartet wird. Wenn ein Port-Scanning-Angriff auf den Computer gestartet wird, verhindert Kaspersky Endpoint Security Datenlecks auf dem Computer. Sie können die Erkennung dieser Angriffstypen deaktivieren, falls einige Ihrer zulässigen Programme Vorgänge ausführen, die für diese Angriffstypen typisch sind. Auf diese Weise können Fehlalarme vermieden werden.
Angreifenden Computer zur Sperrliste hinzufügen für N Minuten	Ist dieses Kontrollkästchen aktiviert, so fügt die Komponente „Schutz vor Netzwerkbedrohungen“ den angreifenden Computer zur Sperrliste hinzu. Das bedeutet, dass die Komponente „Schutz vor Netzwerkbedrohungen“ die Netzwerkverbindung mit dem angreifenden Computer nach dem ersten Netzwerkangriffsversuch für die angegebene Zeitspanne blockiert. Diese Sperre schützt den Computer des Benutzers automatisch vor möglichen zukünftigen Netzwerkangriffen von derselben Adresse aus. Die Sperrliste können Sie im Fenster Netzwerkmonitor ansehen. Kaspersky Endpoint Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.
Ausnahmen	Die Liste enthält IP-Adressen, von denen die Komponente „Schutz vor Netzwerkbedrohungen“ keine Netzwerkangriffe blockiert. Informationen über Netzwerkangriffe von den IP-Adressen, die zur Ausnahmeliste gehören, werden von Kaspersky Endpoint Security nicht in den Bericht aufgenommen.

Schutz vor MAC-Spoofing	Bei einem Angriff vom Typ *MAC-Spoofing* wird die MAC-Adresse eines Netzwerkgeräts (einer Netzwerkkarte) verändert. Dann kann der Angreifer die Daten, die an das Gerät gesendet werden, auf ein anderes Gerät umleiten und auf diese Daten zugreifen. Kaspersky Endpoint Security kann Mac-Spoofing-Angriffe blockieren und solche Angriffe melden

Firewall

Die „Firewall“ blockiert nicht autorisierte Verbindungen mit dem Computer, wenn das Internet oder ein lokales Netzwerk verwendet wird. Die „Firewall“ kontrolliert auch die Netzwerkaktivität der Programme auf dem Computer. Dadurch wird das lokales Unternehmensnetzwerk vor dem Diebstahl persönlicher Daten und anderen Angriffen geschützt. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der *vordefinierten Netzwerkregeln*.

Der Administrationsagent wird für die Interaktion mit Kaspersky Security Center verwendet. Die Firewall erstellt automatisch Netzwerkregeln, die für die ordnungsgemäße Funktion des Programms und des Administrationsagenten erforderlich sind. Dadurch bedingt öffnet die Firewall bestimmte Ports auf dem Computer. Welche Ports geöffnet werden, hängt von der Rolle des Computers ab (z. B. Verteilungspunkt). Weitere Informationen zu den Ports, die auf dem Computer geöffnet werden, finden Sie in der *Hilfe zu Kaspersky Security Center*.

Netzwerkregeln

Sie können die Netzwerkregeln auf folgenden Ebenen anpassen:

- *Regeln für Netzwerkpakete*. Sie dienen zur Definition von Beschränkungen für die Netzwerkpakete, wobei das Programm keine Rolle spielt. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Kaspersky Endpoint Security hat vordefinierte Netzwerkregeln für Pakete mit Lösungen, die von den Kaspersky-Experten empfohlen werden.

- *Netzwerkregeln für das Programm*. Sie dienen zur Definition von Beschränkungen der Netzwerkaktivität eines konkreten Programms. Dabei werden nicht nur die Merkmale des Netzwerkpakets berücksichtigt, sondern auch das konkrete Programm, an das dieses Netzwerkpaket adressiert ist oder welches das Senden dieses Netzwerkpakets initiiert hat.

Die Komponente „Programm-Überwachung“ kontrolliert mithilfe von *Programmrechten* den Zugriff auf Betriebssystemressourcen, Prozesse und persönliche Daten.

Wenn ein Programm zum ersten Mal gestartet wird, führt die „Firewall“ folgende Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.

2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Firewall“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Das Programm wird einer *Sicherheitsgruppe* zugewiesen: Vertrauenswürdig, Schwach beschränkt, Stark beschränkt, Nicht vertrauenswürdig.

Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Netzwerkaktivität des Programms. Für Programme aus der Sicherheitsgruppe „Stark beschränkt“ sind beispielsweise alle Netzwerkverbindungen verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde das Programm nicht verändert, so wendet die Komponente die aktuellen Netzwerkregeln darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Prioritäten der Netzwerkregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Netzwerkaktivität in mehreren Regeln vorkommt, reguliert die „Firewall“ die Netzwerkaktivität nach der Regel mit der höchsten Priorität.

Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme. Sind für eine Art der Netzwerkaktivität gleichzeitig Netzwerkregeln für Pakete und Netzwerkregeln für Programme vorhanden, wird diese Netzwerkaktivität nach den Netzwerkregeln für Pakete verarbeitet.

Netzwerkregeln für Programme funktionieren wie folgt: Eine Netzwerkregel für Programme enthält Zugriffsregeln je nach Netzwerkstatus: *öffentlich*, *lokal*, *vertrauenswürdig*. Zum Beispiel ist für die Sicherheitsgruppe „Stark beschränkt“ standardmäßig jede Netzwerkaktivität eines Programms in Netzwerken mit beliebigem Status verboten. Wenn für ein bestimmtes Programm (übergeordnetes Programm) eine Netzwerkregel vorliegt, werden die untergeordneten Prozesse anderer Programme gemäß der Netzwerkregel des übergeordneten Programms ausgeführt. Gibt es keine Netzwerkregel für ein Programm, so werden die untergeordneten Prozesse gemäß der Regel für den Zugriff auf Netzwerke der Sicherheitsgruppe des Programms ausgeführt.

Beispiel: Sie haben jede Netzwerkaktivität aller Programme für Netzwerke mit beliebigem Status verboten, unter Ausnahme von Browser X. Wenn Browser X (übergeordnetes Programm) die Installation von Browser Y startet (untergeordneter Prozess), erhält Browser Y Zugriff auf das Netzwerk und lädt die erforderlichen Dateien herunter. Nach der Installation sind für Browser Y alle Netzwerkverbindungen verboten, wobei die Einstellungen der Firewall gelten. Um dem Installationsprogramm von Browser Y die Netzwerkaktivität als untergeordneter Prozess zu verbieten, muss eine Netzwerkregel für das Installationsprogramm von Browser Y hinzugefügt werden.

Statusvarianten der Netzwerkverbindungen

Bei der Kontrolle der Netzwerkaktivität kann die „Firewall“ den Status einer Netzwerkverbindung berücksichtigen. Den Status der Netzwerkverbindung erhält Kaspersky Endpoint Security vom Betriebssystem des Computers. Den Status einer Netzwerkverbindung im Betriebssystem legt der Benutzer beim Einrichten der Verbindung fest. Sie können den Status der Netzwerkverbindung in den Einstellungen von Kaspersky Endpoint Security ändern. Dann kontrolliert die „Firewall“ die Netzwerkaktivität anhand des Netzwerkstatus aus den Einstellungen von Kaspersky Endpoint Security, nicht anhand des Status aus dem Betriebssystem.

Für eine Netzwerkverbindung sind folgende Statusvarianten vorgesehen:

- **Öffentliches Netzwerk**. Das Netzwerk wird durch Antiviren-Programme, Firewalls oder Filter geschützt (z. b. WLAN in einem Café). Für den Benutzer eines Computers, der mit einem solchen Netzwerk verbunden ist, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Auch Drittnutzer erhalten über gemeinsame Ordner oder Fernzugriff keinen Zugang zu Informationen auf dem Desktop Ihres Computers. Die Firewall filtert die Netzwerkaktivität für jedes Programm nach den für dieses Programm vorhandenen Netzwerkregeln.

  Das Internet erhält von der Firewall standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.

- **Lokales Netzwerk**. Netzwerk für Benutzer, für die der Zugriff auf die Dateien und Drucker dieses Computers beschränkt ist (beispielsweise ein lokales Unternehmensnetzwerk oder ein privates Netzwerk).

- **Vertrauenswürdiges Netzwerk**. Sicheres Netzwerk, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen. Für Netzwerke mit diesem Status erlaubt die Firewall im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.

Einstellungen für die Komponente „Firewall“

Einstellung	Beschreibung
Netzwerkregeln für Pakete	Tabelle der Netzwerkregeln für Pakete. Netzwerkregeln für Pakete werden verwendet, um Netzwerkpakete unabhängig von Programmen einzuschränken. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Die Tabelle enthält vordefinierte Netzwerkregeln für Pakete, die von Kaspersky zum optimalen Schutz des Netzwerkverkehrs für Computer mit dem Betriebssystem Microsoft Windows empfohlen werden. Die Firewall legt für jede Netzwerkregel für Pakete eine bestimmte Ausführungspriorität fest. Die Firewall führt die Netzwerkregeln für Pakete in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln für Pakete stehen (von oben nach unten). Die Firewall sucht eine passende Paket-Netzwerkregel, die zu der Netzwerkverbindung passt, und führt die entsprechende Aktion aus: Die Netzwerkaktivität wird entweder erlaubt oder blockiert. Die Firewall ignoriert alle weiteren Paket-Netzwerkregeln für diese Netzwerkverbindung. Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme.
Netzwerkverbindungen	Diese Tabelle enthält Informationen über Netzwerkverbindungen, welche die Firewall auf dem Benutzercomputer gefunden hat. Das Internet besitzt standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.
Netzwerkregeln	**Anhänge**

	Tabelle der Programme, die von der Komponente „Firewall“ kontrolliert werden. Die Programme sind auf Sicherheitsgruppen verteilt. Die Sicherheitsgruppe entscheidet über die Rechte, die Kaspersky Endpoint Security zur Kontrolle der Netzwerkaktivität von Programmen verwendet. Sie können ein Programm aus einer Liste aller Programme auswählen, die auf den Computern installiert sind, für welche die Richtlinie gilt, und das Programm einer Sicherheitsgruppe zuweisen. **Netzwerkregeln** Tabelle der Netzwerkregeln für Programme, die zu einer Sicherheitsgruppe gehören. Nach diesen Regeln reguliert die „Firewall“ die Netzwerkaktivität von Programmen. Die Tabelle enthält die vordefinierten Netzwerkregeln, die von den Kaspersky-Experten empfohlen werden. Diese Netzwerkregeln dienen dem optimalen Schutz des Netzwerkverkehrs. Die vordefinierten Netzwerkregeln können nicht gelöscht werden.

Schutz vor modifizierten USB-Geräten

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird. Infolgedessen kann der Virus unter Ihrem Benutzerkonto Befehle ausführen, um z. B. Malware herunterzuladen.

Die Komponente „Schutz vor modifizierten USB-Geräten“ verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.

Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (falls diese verfügbar ist) einen vom Programm generierten digitalen Code einzugeben (siehe nachstehende Abbildung). Dieser Vorgang heißt Autorisierung der Tastatur.

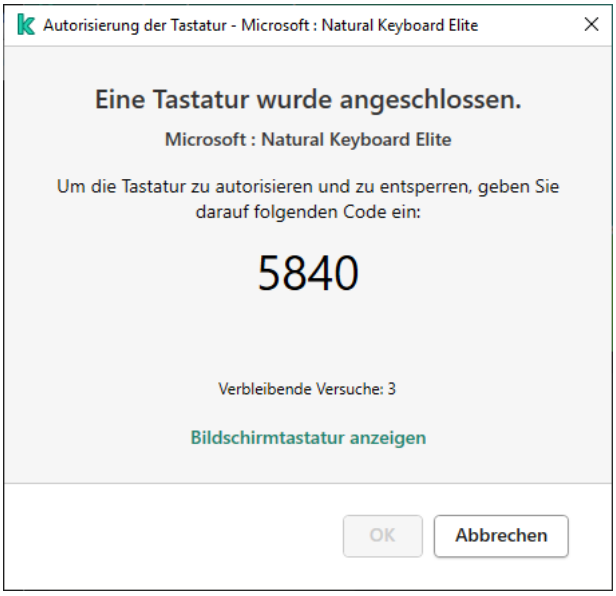
Wurde der richtige Code eingegeben, so speichert das Programm die Identifikationsparameter (VID/PID der Tastatur und Nummer des Ports, über den die Tastatur verbunden ist) in der Liste der autorisierten Tastaturen. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, ist keine Autorisierung erforderlich.

Wenn eine autorisierte Tastatur über einen anderen USB-Port mit dem Computer verbunden wird, fragt das Programm erneut nach der Autorisierung.

Wurde der digitale Code falsch eingegeben, so generiert das Programm einen neuen Code. Die Anzahl der Eingabeversuche für den digitalen Code ist auf drei beschränkt. Nachdem der digitale Code dreimal falsch eingegeben wurde oder das Fenster **Autorisierung der Tastatur <Name der Tastatur>** geschlossen wurde, blockiert das Programm die Eingabe von dieser Tastatur. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, schlägt das Programm erneut vor, die Autorisierung vorzunehmen.

Das Programm erlaubt die Verwendung einer autorisierten Tastatur. Eine Tastatur, die nicht autorisiert wurde, wird blockiert.

Die Komponente „Schutz vor modifizierten USB-Geräten“ wird nicht standardmäßig installiert. Wenn Sie die Komponente „Schutz vor modifizierten USB-Geräten“ benötigen, können Sie die Komponente entweder vor der Programminstallation in den Eigenschaften des Installationspakets hinzufügen oder nach der Programminstallation die Auswahl der Programmkomponenten ändern.



Autorisierung der Tastatur

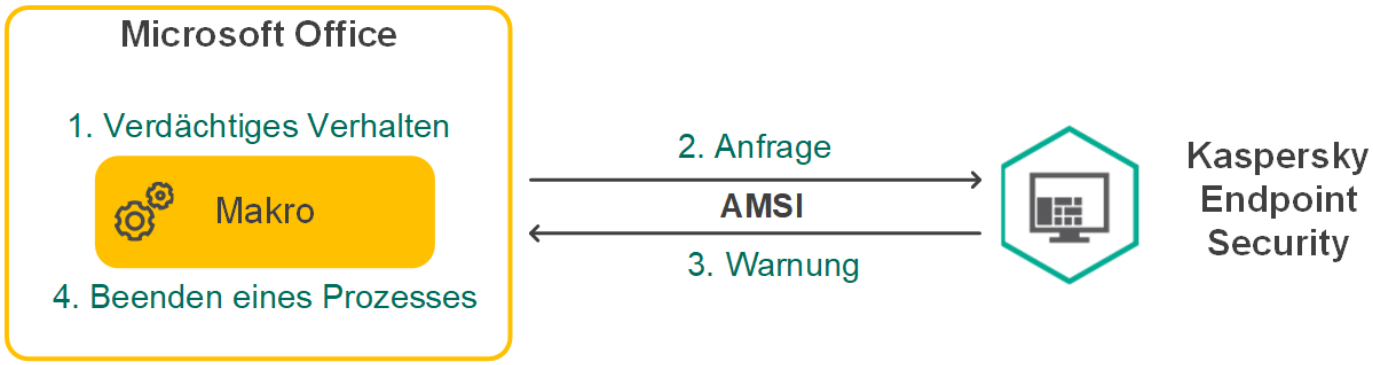
Einstellungen für die Komponente „Schutz vor modifizierten USB-Geräten“

Einstellung	Beschreibung
Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten	Ist das Kontrollkästchen aktiviert, so verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung eines USB-Geräts, von dem aus der Autorisierungscode nicht eingegeben werden kann.

AMSI-Schutz

Die AMSI-Schutz-Komponente ist für die Unterstützung der Microsoft-Schnittstelle für „Antimalware Scan Interface“ vorgesehen. Mithilfe *Schnittstelle für Antimalware Scan Interface (AMSI)* können Drittherstellter-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Endpoint Security senden und Untersuchungsergebnisse für diese Objekte erhalten. Drittherstellter-Anwendungen können z. B. Microsoft-Office-Programme sein (siehe folgende Abb.). Details über die AMSI-Schnittstelle finden Sie in der *Dokumentation von Microsoft*.

Die Funktion von „AMSI-Schutz“ ist darauf beschränkt, eine Bedrohung zu erkennen und eine Drittanbieterprogramm über die gefundene Bedrohung zu benachrichtigen. Nachdem eine Drittherstellter-Anwendung über eine Bedrohung benachrichtigt wurde, verbietet sie die Ausführung schädlicher Aktionen (z. B. Programm beenden).



Beispiel für die Funktionsweise von AMSI

Die Komponente „AMSI-Schutz“ kann die Anfrage eines Drittanbieterprogramms zurückweisen. Dies ist beispielsweise möglich, wenn dieses Programm die maximale Anzahl von Anfragen innerhalb des festgelegten Zeitraums erreicht hat. Kaspersky Endpoint Security sendet Informationen über die Ablehnung der Anfrage einer Dritthersteller-Anwendung an den Administrationsserver. Die Komponente „AMSI-Schutz“ weist Anfragen von jenen Drittanbieterprogrammen nicht zurück, für die das Kontrollkästchen **Interaktion mit AMSI-Provider nicht blockieren** aktiviert ist.

“AMSI-Schutz“ ist für die folgenden Betriebssysteme für Workstations und Server verfügbar:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2019 Essentials / Standard / Datacenter.

Einstellungen der Komponente „AMSI-Provider”

Einstellung	Beschreibung
Archive untersuchen	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.
Programmpakete untersuchen	Dieses Kontrollkästchen aktiviert / deaktiviert die Untersuchung der Programmpakete von Drittherstellern.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Große zusammengesetzte Dateien nicht entpacken	Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe. Unabhängig vom Status dieses Kontrollkästchens untersucht Kaspersky Endpoint Security große Dateien, die aus Archiven extrahiert werden.

Exploit-Prävention

Die Komponente „Exploit-Prävention“ überwacht Programmcode, der mithilfe eines Exploits Schwachstellen eines Computers ausnutzt, um dadurch Administratorrechte zu erhalten oder schädliche Aktionen auszuführen. Exploits können beispielsweise einen Angriff mit Überlauf der Zwischenablage verwenden. Dazu sendet der Exploit große Datenvolumen an ein verwundbares Programm. Bei der Verarbeitung dieser Daten führt das verwundbare Programm schädlichen Code aus. Aufgrund dieses Angriffs kann der Exploit eine nicht autorisierte Installation von Schadsoftware starten.

Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer ausgeführt wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei oder informiert den Benutzer.

Einstellungen der Komponente „Exploit-Prävention“

Einstellung	Beschreibung
Wenn ein Exploit erkannt wurde	• **Vorgang blockieren**. Ist diese Variante ausgewählt, so blockiert Kaspersky Endpoint Security bei einem Exploit-Fund die Aktionen dieses Exploits. • **Informieren** Ist diese Variante ausgewählt und ein Exploit wird gefunden, so blockiert Kaspersky Endpoint Security die Exploit-Aktionen nicht und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.
Schutz für den Arbeitsspeicher von Systemprozessen aktivieren	Ist dieser Schalter aktiviert, so blockiert Kaspersky Endpoint Security Drittanbieter-Prozesse, die versuchen, auf den Arbeitsspeicher von Systemprozessen zuzugreifen.

Verhaltensanalyse

Die Komponente „Verhaltensanalyse“ empfängt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt andere Schutzkomponenten mit diesen Informationen, um deren Effektivität zu erhöhen.

Die Komponente „Verhaltensanalyse“ verwendet Vorlagen für gefährliches Programmverhalten. Stimmt die Aktivität eines Programms mit einer der Aktivitäten aus den Vorlagen für gefährliches Verhalten überein, so führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Endpoint Security, die auf Vorlagen für gefährliches Verhalten beruht, bietet einen proaktiven Computerschutz.

Einstellungen der Komponente „Verhaltensanalyse“

Einstellung	Beschreibung
Wenn schädliche Programmaktivität erkannt wird	• **Datei löschen**. Ist diese Variante ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an. • **Programm beenden**. Ist diese Variante ausgewählt, so beendet Kaspersky Endpoint Security beim Fund einer schädlichen Programmaktivität die betreffende Anwendung. • **Informieren** Ist diese Variante ausgewählt und es wird eine schädliche Programmaktivität erkannt, so beendet Kaspersky Endpoint Security dieses Programm nicht und fügt Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.
Schutz vor der externen	Ist der Schalter aktiviert, so analysiert Kaspersky Endpoint Security die Aktivität in gemeinsamen Ordnern. Falls die Aktivität mit einer Vorlage für gefährliches Verhalten

Verschlüsselung von gemeinsamen Ordnern aktivieren	übereinstimmt, das für eine externe Verschlüsselung charakteristisch ist, so führt Kaspersky Endpoint Security die ausgewählte Aktion aus. Kaspersky Endpoint Security schützt nur jene Dateien vor ferngesteuerten Verschlüsselungsversuchen, die sich auf Datenträgern mit NTFS-Dateisystem befinden und nicht mit einem EFS-System verschlüsselt wurden. • **Informieren** Wenn diese Variante ausgewählt ist und es wird erkannt, dass versucht wird, Dateien in gemeinsamen Ordnern zu ändern, so fügt Kaspersky Endpoint Security Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu. • **Verbindung blockieren** Ist diese Variante ausgewählt und es wird ein Versuch erkannt, Dateien in gemeinsamen Ordnern zu ändern, so blockiert Kaspersky Endpoint Security die Netzwerkaktivität des Computers, der die Änderung initiiert hat, und erstellt Backup-Kopien der veränderten Dateien. Ist die Komponente „Rollback von schädlichen Aktionen“ aktiviert und die Variante **Verbindung blockieren** ausgewählt, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.
Verbindung blockieren für n Minuten	Zeitraum, für den Kaspersky Endpoint Security die Netzwerkaktivität eines Remote-Computers blockieren soll, der versucht, gemeinsame Ordner zu verschlüsseln.
Ausnahmen	Liste der Computer, deren Verschlüsselungsversuche für gemeinsame Ordner nicht überwacht werden. Damit die Ausnahmeliste funktioniert, mit der Computer aus dem Schutz gemeinsamer Ordner vor externer Verschlüsselung ausgeschlossen werden, muss die Überwachung von Anmeldeereignissen am System in der Windows-Sicherheitsüberwachungsrichtlinie aktiviert werden. Die Überwachung von Anmeldeereignissen am System ist standardmäßig deaktiviert. Details über die Windows-Sicherheitsüberwachungsrichtlinie finden Sie auf der *Microsoft-Website*).

Programm-Überwachung

Die Komponente „Programm-Überwachung“ (HIPS, Host Intrusion Prevention System) hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken und des Cloud-Dienstes Kaspersky Security Network

Die Komponente kontrolliert Programme mithilfe von *Programmrechten*. Programmrechte beinhalten die folgenden Zugriffseinstellungen:

- Zugriff auf Betriebssystemressourcen (z. B. Autostart-Einstellungen und Registrierungsschlüssel)
- Zugriff auf persönliche Daten (z. B. auf Dateien und Programme)

Die Netzwerkaktivität von Programmen wird von der Firewall mithilfe von *Netzwerkregeln* kontrolliert.

Wenn ein Programm zum ersten Mal gestartet wird, führt die Komponente „Programm-Überwachung“ die folgenden Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.
2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Programm-Überwachung“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Das Programm wird einer *Sicherheitsgruppe* zugewiesen: Vertrauenswürdig, Schwach beschränkt, Stark beschränkt, Nicht vertrauenswürdig.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Aktionen des Programms. Für Programme aus der Sicherheitsgruppe „Stark beschränkt“ ist beispielsweise der Zugriff auf Module des Betriebssystems verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde ein Programm nicht verändert, so wendet die Komponente die aktuellen Rechte für Programme darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Einstellungen der Komponente „Programm-Überwachung“

Einstellung	Beschreibung
Rechte für Programme	**Programme** Tabelle der Programme, die von der Komponente „Programm-Überwachung“ kontrolliert werden. Die Programme sind auf Sicherheitsgruppen verteilt. Die Sicherheitsgruppe entscheidet über die Rechte, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Sie können ein Programm aus einer Liste aller Programme auswählen, die auf den Computern installiert sind, für welche die Richtlinie gilt, und das Programm einer Sicherheitsgruppe zuweisen. Die folgenden Tabellen enthalten die Zugriffsrechte von Programmen: • **Dateien und Systemregistrierung**. Diese Tabelle enthält die Zugriffsrechte von Programmen, die zu einer Sicherheitsgruppe gehören. Die Rechte beziehen sich auf

	die Ressourcen des Betriebssystems und auf persönliche Daten. • **Rechte**. Diese Tabelle enthält die Zugriffsrechte von Programmen, die zu einer Sicherheitsgruppe gehören. Die Rechte beziehen sich auf die Prozesse und Ressourcen des Betriebssystems. • **Netzwerkregeln**. Tabelle der Netzwerkregeln für Programme, die zu einer Sicherheitsgruppe gehören. Nach diesen Regeln reguliert die Firewall die Netzwerkaktivität von Programmen. Die Tabelle enthält die vordefinierten Netzwerkregeln, die von den Kaspersky-Experten empfohlen werden. Diese Netzwerkregeln dienen dem optimalen Schutz des Netzwerkverkehrs. Die vordefinierten Netzwerkregeln können nicht gelöscht werden.
Geschützte Ressourcen	**Name** Die Tabelle enthält Computerressourcen, die nach Kategorien angeordnet sind. Die Komponente „Programm-Überwachung“ kontrolliert den Zugriff anderer Programme auf die Ressourcen aus dieser Tabelle. Eine Ressource kann sein: Registrierungskategorie, Datei, Ordner oder Registrierungsschlüssel. **Programme** Tabelle der Programme, die von der Komponente „Programm-Überwachung“ für die ausgewählte Ressource kontrolliert werden. Die Programme sind auf Sicherheitsgruppen verteilt. Die Sicherheitsgruppe entscheidet über die Rechte, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet.
Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden	Sicherheitsgruppe, in die Kaspersky Endpoint Security die Programme verschiebt, die vor Kaspersky Endpoint Security gestartet werden.
Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren	Ist das Kontrollkästchen aktiviert, so aktualisiert die Komponente „Programm-Überwachung“ die Rechte von bisher unbekannten Programmen unter Verwendung der Datenbank von Kaspersky Security Network.
Programmen mit digitaler Signatur vertrauen	Ist dieses Kontrollkästchen aktiviert, so weist die Komponente „Programm-Überwachung“ die Programme, die eine digitale Signatur eines vertrauenswürdigen Herstellers besitzen, der Gruppe „Vertrauenswürdig“ zu. *Vertrauenswürdige Hersteller* sind Softwareanbieter, denen Kaspersky vertraut. Sie können ein Herstellerzertifikat auch manuell zum Speicher für vertrauenswürdige Zertifikate hinzufügen. Ist das Kontrollkästchen deaktiviert, so stuft die Komponente „Programm-Überwachung“ solche Programme nicht als vertrauenswürdig ein und weist sie anhand anderer Kriterien zu den Sicherheitsgruppen zu.
Rechte für Programme löschen, wenn nicht gestartet seit n Tagen	Ist das Kontrollkästchen aktiviert, so löscht Kaspersky Endpoint Security automatisch die Informationen über das Programm (Sicherheitsgruppe, Zugriffsrechte), wenn die folgenden Bedingungen erfüllt sind: • Sie haben das Programm einer Sicherheitsgruppe zugeordnet oder die Zugriffsrechte manuell angepasst. • Das Programm wurde innerhalb des festgelegten Zeitraums nicht gestartet.

	Wenn die Sicherheitsgruppe und die Programmrechte automatisch festgelegt wurden, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 30 Tagen. Es ist nicht möglich, die Speicherdauer für Informationen über ein Programm zu ändern oder das automatische Löschen zu deaktivieren. Wenn dieses Programm zum nächsten Mal gestartet wird, untersucht Kaspersky Endpoint Security das Programm wie beim ersten Start.
Sicherheitsgruppe für Programme, die keiner anderen Gruppe zugewiesen werden konnten	Mit den Elementen dieser Dropdown-Liste wird festgelegt, welcher Sicherheitsgruppe Kaspersky Endpoint Security ein unbekanntes Programm zuordnen soll. Sie können eines der folgenden Elemente wählen: • **Schwach beschränkt**. • **Stark beschränkt**. • **Nicht vertrauenswürdig**.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- **Dateiaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht ausführbare Dateien, die von Schadsoftware erstellt wurden (auf allen Datenträgern, außer auf Netzlaufwerken).
  - löscht ausführbare Dateien, die von Programmen erstellt wurden, in welche Schadsoftware eingedrungen ist.
  - stellt Dateien wieder her, die von Schadsoftware verändert oder gelöscht wurden.

  Die Funktionalität zur Wiederherstellung von Dateien besitzt bestimmte Beschränkungen.

- **Aktivität der Registrierung**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.
  - stellt Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden, nicht wieder her.

- **Systemaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - beendet Prozesse, die von Schadsoftware gestartet wurden.
  - beendet Prozesse, in die Schadsoftware eingedrungen ist.

- stellt Prozesse, die von Schadsoftware beendet wurden, nicht wieder her.

- **Netzwerkaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - verbietet die Netzwerkaktivität von Schadsoftware.
  - verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback von Schadsoftware-Aktionen kann entweder von der Komponente Schutz vor bedrohlichen Dateien, Verhaltensanalyse oder bei einer Untersuchung auf Viren gestartet werden.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich eine eng eingeschränkte Auswahl an Daten. Ein Rollback hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und die Integrität der Daten auf Ihrem Computer.

Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. Wenn Sie an Kaspersky Security Network teilnehmen, erhält das Programm Kaspersky Endpoint Security von den KSN-Diensten Informationen über die Kategorie und die Reputation untersuchter Dateien, sowie Informationen über die Reputation untersuchter Webadressen.

Die Verwendung von Kaspersky Security Network ist freiwillig. Das Programm schlägt während der Erstkonfiguration des Programms vor, KSN zu verwenden. Die KSN-Nutzung kann jederzeit begonnen oder beendet werden.

Ausführliche Informationen darüber, welche Informationen an Kaspersky gesendet werden und wie statistische Informationen gespeichert und gelöscht werden, finden Sie in der „Erklärung zu Kaspersky Security Network“ und auf der Website von Kaspersky. Die Datei ksn_<Sprach-ID>.txt mit dem Text der Vereinbarung über Kaspersky Security Network ist im Lieferumfang des Programms enthalten.

Um die Auslastung der KSN-Server zu reduzieren, kann Kaspersky Programm-Updates veröffentlichen, welche die Zugriffsmöglichkeit auf das Kaspersky Security Network vorübergehend deaktivieren oder teilweise einschränken. In diesem Fall wird auf der lokalen Programmoberfläche der KSN-Verbindungsstatus *Aktiviert mit Einschränkungen* angezeigt.

KSN-Infrastruktur

Kaspersky Endpoint Security unterstützt die folgenden KSN-Infrastruktur-Lösungen:

- Die Lösung *Global KSN* wird von den meisten Kaspersky-Programmen verwendet. Die KSN-Teilnehmer erhalten von Kaspersky Security Network Informationen und senden an Kaspersky bestimmte Daten über Objekte, die auf dem Benutzercomputer gefunden wurden. Auf diese Weise können die Daten zusätzlich durch die Kaspersky-Analytiker untersucht werden, und die Reputations- und Statistik-Datenbanken von Kaspersky Security Network werden ergänzt.

- Die Lösung *Private KSN* ermöglicht Benutzern den Zugriff auf die Reputations-Datenbanken und auf andere statistische Daten, ohne dabei Daten von den Benutzercomputern an KSN zu senden. Auf diesen Computern müssen das Programm Kaspersky Endpoint Security oder andere Kaspersky-Programme installiert sein. Private KSN wurde für Unternehmenskunden entwickelt, die z. B. aus folgenden Gründen keine Möglichkeit zur Teilnahme an Kaspersky Security Network haben:

  - Lokale Arbeitsplätze haben keinen Internetzugriff.

  - Es ist gesetzlich verboten oder durch die Unternehmenssicherheit beschränkt, beliebige Daten in andere Länder oder aus dem lokalen Unternehmensnetzwerk heraus zu senden.

Kaspersky Security Center verwendet standardmäßig Global KSN. Die Verwendung von Private KSN können Sie in der Verwaltungskonsole (MMC), in der Kaspersky Security Center 12 Web Console und über die Befehlszeile anpassen. Es ist nicht möglich, die Verwendung von Private KSN in Kaspersky Security Center Cloud Console anzupassen.

Details über die Funktionsweise von Private KSN finden Sie in der *Dokumentation zu Kaspersky Private Security Network*.

KSN Proxy

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können zur Interaktion mit KSN den Dienst KSN Proxy verwenden.

Der Dienst KSN Proxy bietet folgende Möglichkeiten:

- Ein Benutzercomputer kann Anfragen an KSN ausführen und Informationen an KSN übertragen, auch wenn er keinen direkten Internetzugang besitzt.

- Der Dienst KSN Proxy übernimmt die Zwischenspeicherung von aufbereiteten Daten. Dadurch wird der Verbindungskanal zu dem externen Netzwerk entlastet und der Empfang angeforderter Informationen durch den Benutzercomputer wird beschleunigt.

Ausführliche Informationen über den Dienst KSN Proxy finden Sie in der *Hilfe zu Kaspersky Security Center*.

Einstellungen für „Kaspersky Security Network"

Einstellung	Beschreibung
Erweiterten KSN-Modus aktivieren	Im *erweiterten KSN-Modus* überträgt Kaspersky Endpoint Security zusätzliche Daten an Kaspersky. Unabhängig vom Zustand des Schalters verwendet Kaspersky Endpoint Security KSN für die Erkennung von Bedrohungen.
Cloud-Modus aktivieren	*Cloud-Modus* – Modus des Programms, in dem Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken verwendet. Das Funktionieren des Programms mit einer eingeschränkten Version der Antiviren-Datenbanken wird durch Kaspersky Security Network gewährleistet. Mithilfe der eingeschränkten Version der Antiviren-Datenbanken kann die Auslastung des Computer-Arbeitsspeichers etwa um die Hälfte reduziert werden. Wenn Sie nicht an Kaspersky Security Network teilnehmen oder der Cloud-Modus deaktiviert ist, lädt Kaspersky Endpoint Security die komplette Version der Antiviren-Datenbanken von den Kaspersky-Servern herunter. Ist der Schalter aktiviert, so verwendet Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken. Dadurch werden die Betriebssystemressourcen entlastet.

	Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update eine eingeschränkte Version der Antiviren-Datenbanken herunter. Ist der Schalter deaktiviert, so verwendet Kaspersky Endpoint Security die vollständige Version der Antiviren-Datenbanken. Nachdem das Kontrollkästchen deaktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Antiviren-Datenbanken herunter.
Computerstatus, wenn KSN-Server nicht verfügbar sind *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Mit den Elementen dieser Dropdown-Liste wird der Computerstatus in Kaspersky Security Center für den Fall festgelegt, dass die KSN-Server nicht verfügbar sind.
KSN-Proxy verwenden *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security den Dienst KSN Proxy. Die Einstellungen für den Dienst KSN Proxy können Sie in den Eigenschaften des Administrationsservers anpassen.
KSN-Server verwenden, wenn KSN Proxy nicht erreichbar ist *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security die KSN-Server, wenn der Dienst KSN Proxy nicht verfügbar ist. Die KSN-Server können sich bei Verwendung von Global KSN auf der Seite von Kaspersky befinden, oder auf Servern von Drittherstellern, wenn Private KSN verwendet wird.

Web-Kontrolle

Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch lässt sich Datenverkehr einsparen und die zweckentfremdete Nutzung der Arbeitszeit reduzieren. Wenn ein Benutzer versucht, eine Website zu öffnen, auf den die „Web-Kontrolle“ den Zugriff beschränkt, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).

Kaspersky Endpoint Security kontrolliert nur den HTTP- und HTTPS-Datenverkehr.

Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

Methoden zur Verwaltung des Zugriffs auf Websites

Mithilfe der „Web-Kontrolle“ kann der Zugriff auf Websites wie folgt angepasst werden:

- **Website-Kategorie**. Eine Kategorisierung der Websites wird gewährleistet vom Cloud-Dienst für Kaspersky Security Network, von der heuristischen Analyse und von der Datenbank für unbekannte Websites (im Lieferumfang des Programms enthalten). So können Sie z. B. den Benutzerzugriff auf die Kategorie „Soziale Netzwerke“ oder auf andere Kategorien beschränken.

- **Datentyp**. Sie können für Benutzer den Zugriff auf die Daten auf einer Website beschränken und beispielsweise Grafiken verbergen. Kaspersky Endpoint Security ermittelt den Datentyp aufgrund des Dateiformats, nicht nach der Erweiterung.

  Dateien in Archiven werden durch Kaspersky Endpoint Security nicht untersucht. Befinden sich beispielsweise Bilddateien in einem Archiv, so ermittelt Kaspersky Endpoint Security den Datentyp „Archive“, nicht „Bilddateien“.

- **Bestimmte Adresse**. Sie können eine Webadresse eingeben oder Masken verwenden.

Sie können gleichzeitig mehrere Methoden verwenden, um den Zugriff auf Websites zu regulieren. Der Zugriff auf den Datentyp „Dateien für Office-Programme“ lässt sich beispielsweise nur für die Website-Kategorie „Web-E-Mail“ beschränken.

Regeln für den Zugriff auf Websites

Die „Web-Kontrolle“ verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Sie können eine Regel für den Zugriff auf Websites wie folgt zusätzlich anpassen:

- Benutzer, für welche die Regel gilt.

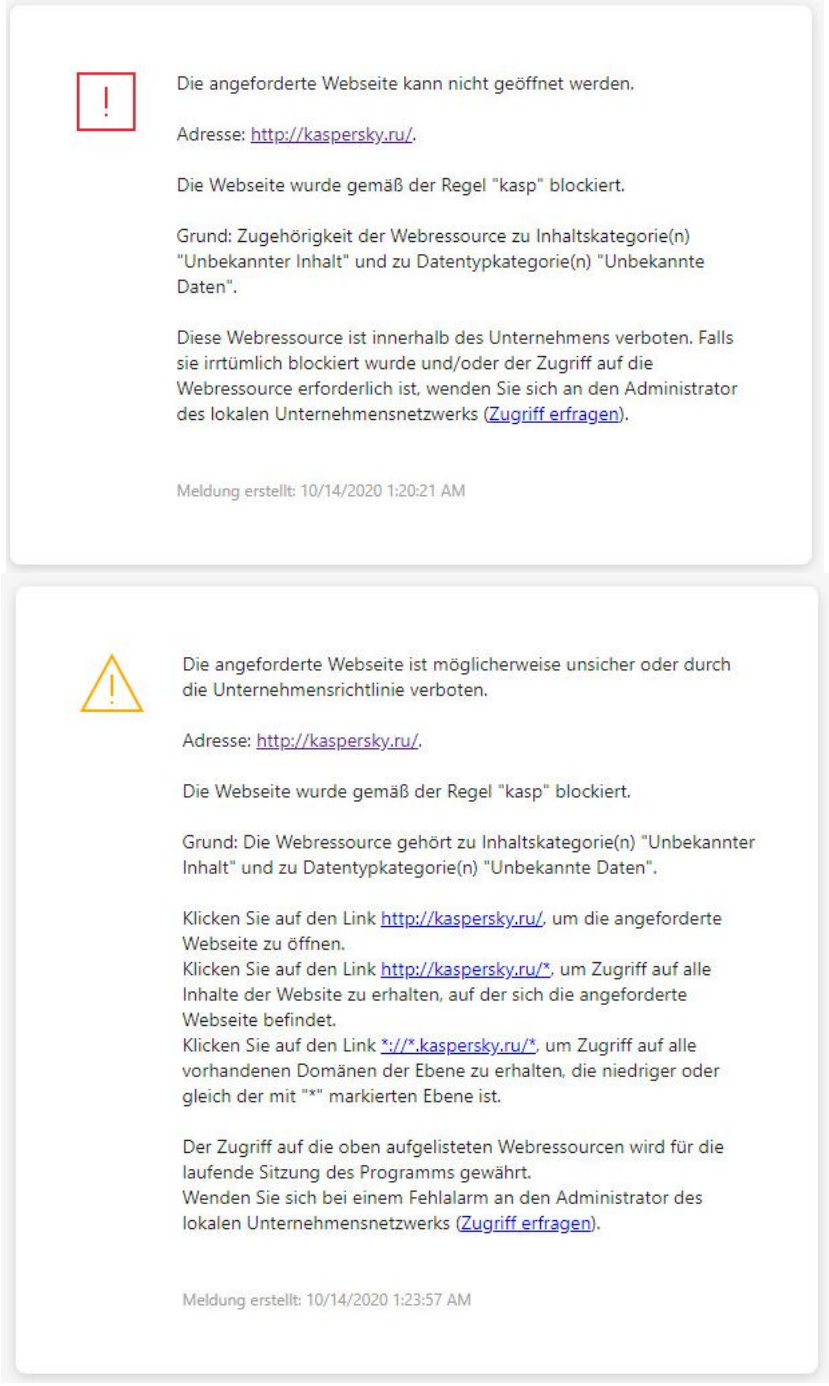
  Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- Zeitplan für die Regel.

  Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Prioritäten für Zugriffsregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Website in mehreren Regeln vorkommt, reguliert die „Web-Kontrolle“ den Zugriff auf die Website nach der Regel mit der höchsten Priorität. Es kann beispielsweise vorkommen, dass Kaspersky Endpoint Security ein Unternehmensportal als soziales Netzwerk betrachtet. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „Soziale Netzwerke“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Unternehmens-Web-Portal muss eine höhere Priorität haben als die Zugriffsregel für soziale Netzwerke.



Benachrichtigungen der „Web-Kontrolle"

Einstellungen der Komponente „Web-Kontrolle"

Einstellung	Beschreibung
Regeln für den Zugriff auf Webressourcen	Liste der Zugriffsregeln für Webressourcen. Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Website in mehreren Regeln vorkommt, reguliert die „Web-Kontrolle" den Zugriff auf die Website nach der Regel mit der höchsten Priorität.
Standardregel	Eine *Standardregel* ist eine Regel für den Zugriff auf Webressourcen, für die keine der Regeln gilt. Folgende Varianten stehen zur Auswahl: • **Alle erlauben, die nicht in der Regelliste angegeben sind**, auch bekannt als Denylist-Modus für verbotene Websites. • **Alle verbieten, die nicht in der Regelliste angegeben sind**, die auch als Allowlist-Modus für erlaubte Websites bekannt ist.

Vorlagen für Nachrichten	• **Warnung** Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt. • **Nachricht zum Blockieren**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die den Zugriff auf eine Webressource blockiert. • **Nachricht an den Administrator**. Das Eingabefeld enthält eine Vorlage für die Meldung, die an den Administrator des lokalen Firmennetzwerks zu senden ist, wenn der Zugriff auf eine Webressource nach Meinung des Benutzers irrtümlich blockiert wurde.
Daten über den Besuch erlaubter Seiten protokollieren	Kaspersky Endpoint Security protokolliert Daten über den Besuch aller Websites, einschließlich erlaubter Websites. Kaspersky Endpoint Security sendet Ereignisse an Kaspersky Security Center, an den lokalen Bericht für Kaspersky Endpoint Security, an das Windows-Ereignisprotokoll. Für die Überwachung der Internetaktivitäten des Benutzers müssen die Einstellungen für die Ereignisspeicherung angepasst werden. Die Überwachung der Internetaktivitäten des Benutzers kann bei einer Entschlüsselung des HTTPS-Datenverkehrs mehr Computer-Ressourcen erfordern.

Gerätekontrolle

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die „Gerätekontrolle“ verwaltet den Zugriff von Benutzern auf die Geräte, die installiert oder mit dem Computer verbunden sind (z. B. auf Festplatten, Kamera oder WLAN-Modul). Bei einer Verbindung mit diesen Geräten kann der Computer so vor einer Infektion geschützt werden, und Datenverlust oder Datendiebstahl lassen sich verhindern.

Ebenen für den Zugriff auf Geräte

Die „Gerätekontrolle“ verwaltet den Zugriff auf folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger, CD/DVD-Laufwerke.
  Sie können den Zugriff auf Geräte wie folgt anpassen:
  - Erlauben – .
  - Verbieten – .
  - Von der Schnittstelle abhängig (unter Ausnahme von WLAN) – .
  - Block mit Ausnahmen (nur WLAN) – .

- **Schnittstellen**. Mithilfe einer *Verbindungsschnittstelle* können Geräte mit einem Computer verbunden werden (z. B. via USB oder FireWire). Auf diese Weise können Sie beispielsweise für alle Geräte eine Verbindung über USB beschränken.

  Sie können den Zugriff auf Geräte wie folgt anpassen:

  - Erlauben – ✓.
  - Verbieten – ⊘.

- **Vertrauenswürdige Geräte**. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

  Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

  - **Geräte nach ID**. Jedes Gerät besitzt eine einmalige ID (engl. Hardware ID – HWID). Die ID finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Beispiel für eine Geräte-ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten.
  - **Geräte nach Modell**. Jedes Gerät besitzt eine einmalige Hersteller-ID (engl. Vendor ID – VID) und eine Produkt-ID (engl. Product ID – PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Eigenschaften des Gerätes. Vorlage für die Eingabe einer VID und PID: `VID_1234&PID_5678`. Es bietet sich an, Geräte mithilfe des Modells hinzuzufügen, wenn Sie in Ihrem Unternehmen Geräte eines bestimmten Modells verwenden. Dadurch können Sie alle Geräte dieses Modells hinzufügen.
  - **Geräte nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs haben, können Sie eine Maske verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.
  - **Geräte nach Modellmaske**. Wenn Sie mehrere Geräte mit ähnlichen VID oder PID verwenden (beispielsweise Geräte desselben Herstellers), können Sie die Geräte mithilfe einer Maske zur Liste der vertrauenswürdigen Geräte hinzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC & PID_ *`.

Die „Gerätekontrolle“ verwendet *Zugriffsregeln*, um den Zugriff von Benutzern auf Geräte zu regulieren. Außerdem kann die „Gerätekontrolle“ Ereignisse über die Verbindung/Trennung von Geräten speichern. Damit Ereignisse gespeichert werden, müssen Sie in der Richtlinie das Senden von Ereignissen anpassen.

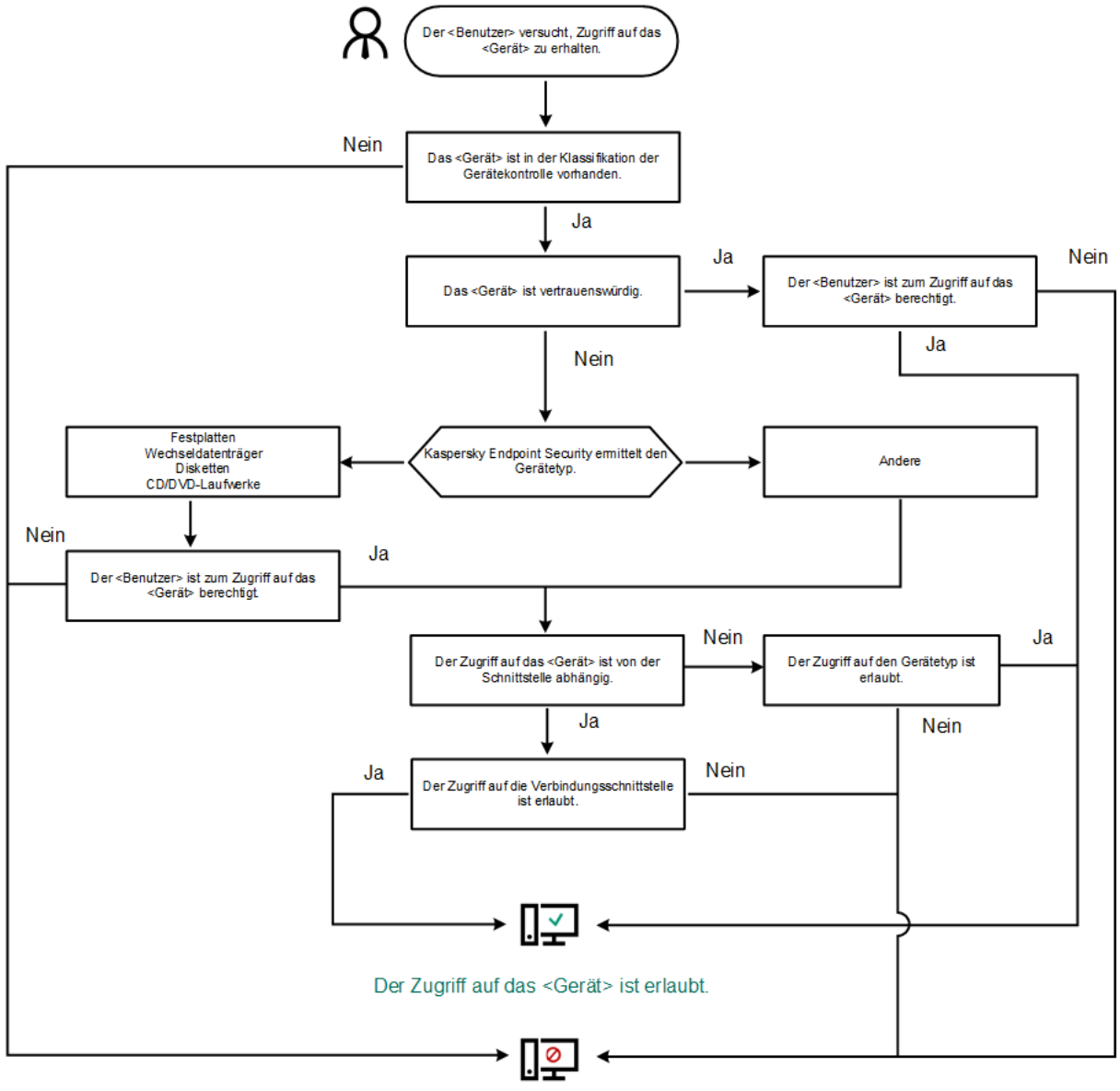
Falls der Zugriff auf das Gerät von der Schnittstelle abhängig ist (Status ◔), werden Ereignisse über die Verbindung/Trennung des Geräts nicht von Kaspersky Endpoint Security gespeichert. Damit das Programm Kaspersky Endpoint Security Ereignisse über die Verbindung/Trennung des Geräts speichert, erlauben Sie den Zugriff auf den entsprechenden Gerätetyp (Status ✓) oder fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

Wird mit dem Computer ein Gerät verbunden, auf das der Zugriff von der „Gerätekontrolle“ verboten ist, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Benachrichtigung an (s. Bild unten).

Benachrichtigung der „Gerätekontrolle"

Algorithmus der „Gerätekontrolle"

Kaspersky Endpoint Security entscheidet über den Zugriff auf ein Gerät, sobald dieses vom Benutzer an den Computer angeschlossen wird (s. folgende Abb.).



Algorithmus der „Gerätekontrolle"

Wenn ein Gerät verbunden ist und der Zugriff erlaubt ist, können Sie die Zugriffsregel ändern und den Zugriff verbieten. Wenn das nächste Mal auf das Gerät zugegriffen wird (Anzeige der Ordnerstruktur, Lesen, Schreiben), blockiert Kaspersky Endpoint Security den Zugriff. Geräte ohne Dateisystem werden erst blockiert, wenn sie zum nächsten Mal mit dem Computer verbunden werden.

Wenn der Benutzer eines Computers, auf dem das Programm Kaspersky Endpoint Security installiert ist, den Zugriff auf ein Gerät angefordert hat, das seiner Meinung nach irrtümlicherweise blockiert wurde, so übermitteln Sie ihm eine Anleitung für die Zugriffsanforderung.

Einstellungen der Komponente „Gerätekontrolle"

Einstellung	Beschreibung
Anfrage auf temporären Zugriff erlauben *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn das Kontrollkästchen aktiviert ist, ist die Schaltfläche **Zugriff erfragen** in der lokalen Programmoberfläche von Kaspersky Endpoint Security verfügbar. Diese Schaltfläche öffnet das Fenster **Zugriff auf ein Gerät erfragen**. In diesem Fenster kann der Benutzer den temporären Zugriff auf ein blockiertes Gerät erfragen.
Geräte und WLANs	Tabelle mit allen verfügbaren Gerätetypen nach der Klassifikation der Komponente „Gerätekontrolle" und dem entsprechenden Zugriffsstatus.
Schnittstellen	Liste aller verfügbaren Schnittstellen nach der Klassifikation der Komponente „Gerätekontrolle" und die entsprechenden Varianten für den Zugriffsstatus.
Vertrauenswürdige Geräte	Liste der vertrauenswürdigen Geräte und Benutzer, denen der Zugriff auf diese Geräte erlaubt ist.
Anti-Bridging	Anti-Bridging verhindert die Erstellung von Netzwerkbrücken und verhindert zu diesem Zweck, dass gleichzeitig mehrere Netzwerkverbindungen für den Computer hergestellt werden. Dadurch kann das Unternehmensnetzwerk vor Angriffen über ungeschützte und nicht autorisierte Netzwerke geschützt werden. Anti-Bridging blockiert die Herstellung mehrerer Verbindungen, wobei die Prioritäten der Geräte berücksichtigt werden. Je weiter oben ein Gerät auf der Liste steht, desto höher ist seine Priorität. Haben eine aktive Verbindung und eine neue Verbindung den gleichen Typ (z. B. WLAN), so blockiert Kaspersky Endpoint Security die aktive Verbindung und erlaubt die Herstellung der neuen Verbindung. Haben eine aktive Verbindung und eine neue Verbindung unterschiedliche Typen (z. B. Netzwerkadapter und WLAN), so blockiert Kaspersky Endpoint Security die Verbindung mit der niedrigeren Priorität und erlaubt die Herstellung der Verbindung mit der höheren Priorität. Anti-Bridging unterstützt die folgenden Gerätetypen: Netzwerkadapter, WLAN und Modem.
Vorlagen für Nachrichten	• **Nachricht zum Blockieren**. Vorlage der Nachricht, die erscheint, wenn der Benutzer auf ein blockiertes Gerät zugreift. Diese Nachricht erscheint auch, wenn der Benutzer versucht, einen Vorgang mit dem Geräteinhalt auszuführen, zu dem dieser Benutzer nicht berechtigt ist. • **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn die

	Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt nach Meinung des Benutzers irrtümlicherweise erfolgt.

Programmkontrolle

Die „Programmkontrolle“ verwaltet den Start von Programmen auf den Benutzercomputern. Dadurch wird ermöglicht, die Sicherheitsrichtlinie des Unternehmens bei der Verwendung von Programmen zu erfüllen. Außerdem reduziert die „Programmkontrolle“ das Risiko einer Infektion des Computers. Dazu wird der Zugriff auf Programme beschränkt.

Die „Programmkontrolle“ wird mit folgenden Schritten angepasst:

1. Programmkategorien erstellen

   Der Administrator erstellt Kategorien für die Programme, die er verwalten möchte. Die Programmkategorien gelten unabhängig von der Administrationsgruppe für alle Computer des Unternehmensnetzwerks. Für die Kategorien können Sie beispielsweise folgende Kriterien verwenden: KL-Kategorie (z. B. *Browser*), Datei-Hash und Programmhersteller.

2. Regeln der „Programmkontrolle“ erstellen.

   Der Administrator erstellt Regeln der „Programmkontrolle“ in der Richtlinie für die Administrationsgruppe. Eine Regel enthält Programmkategorien und einen Startstatus für die Programme aus diesen Kategorien: verboten oder erlaubt.

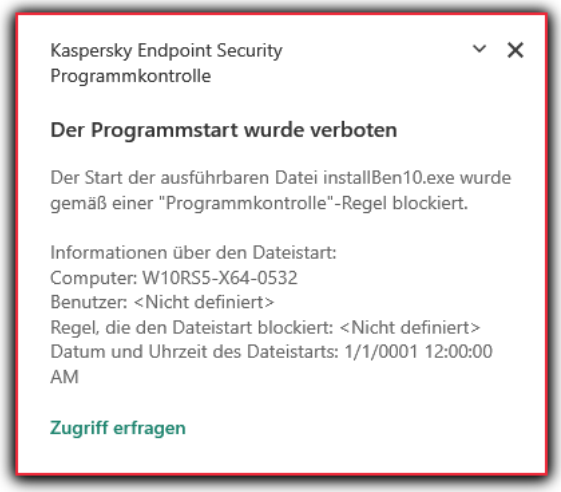
3. Modus der „Programmkontrolle“ auswählen.

   Der Administrator wählt einen Modus für die Arbeit mit den Programmen aus, die zu keiner Regel gehören: Denyliste und Allowliste.

Wenn der Benutzer versucht, ein verbotenes Programm zu starten, blockiert Kaspersky Endpoint Security den Programmstart und zeigt eine Benachrichtigung an (s. Abb. unten).

Die Einstellungen der „Programmkontrolle“ können im *Testmodus* überprüft werden. In diesem Modus führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Der Start von Programmen (auch von verbotenen Programmen) wird erlaubt.
- Beim Start eines verbotenen Programms wird eine entsprechende Benachrichtigung angezeigt und Informationen werden zum Bericht auf dem Benutzercomputer Informationen hinzugefügt.
- Daten über den Start verbotener Programme werden an Kaspersky Security Center gesendet.



Benachrichtigung der „Programmkontrolle"

Modi der „Programmkontrolle"

Die Komponente „Programmkontrolle" bietet zwei Modi:

- **Deny-Liste**. In diesem Modus erlaubt die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" verboten sind.

  Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

- **Allow-Liste**. In diesem Modus verbietet die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" erlaubt und nicht verboten sind.

  Wenn eine extrem genaue Erlaubnisregel für die Programmkontrolle erstellt wurde, verbietet die Komponente den Start aller neuen Programme, die noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet dabei aber die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Programme, die von Benutzern für dienstliche Zwecke benötigt werden.

  Beachten Sie die Tipps für die Anpassung von Regeln der Programmkontrolle im Allowlist-Modus.

Diese Modi für die Programmkontrolle können sowohl auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security als auch mithilfe von Kaspersky Security Center angepasst werden.

Allerdings verfügt Kaspersky Security Center über Tools, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht verfügbar sind und für folgende Aufgaben dienen:

- Programmkategorien erstellen

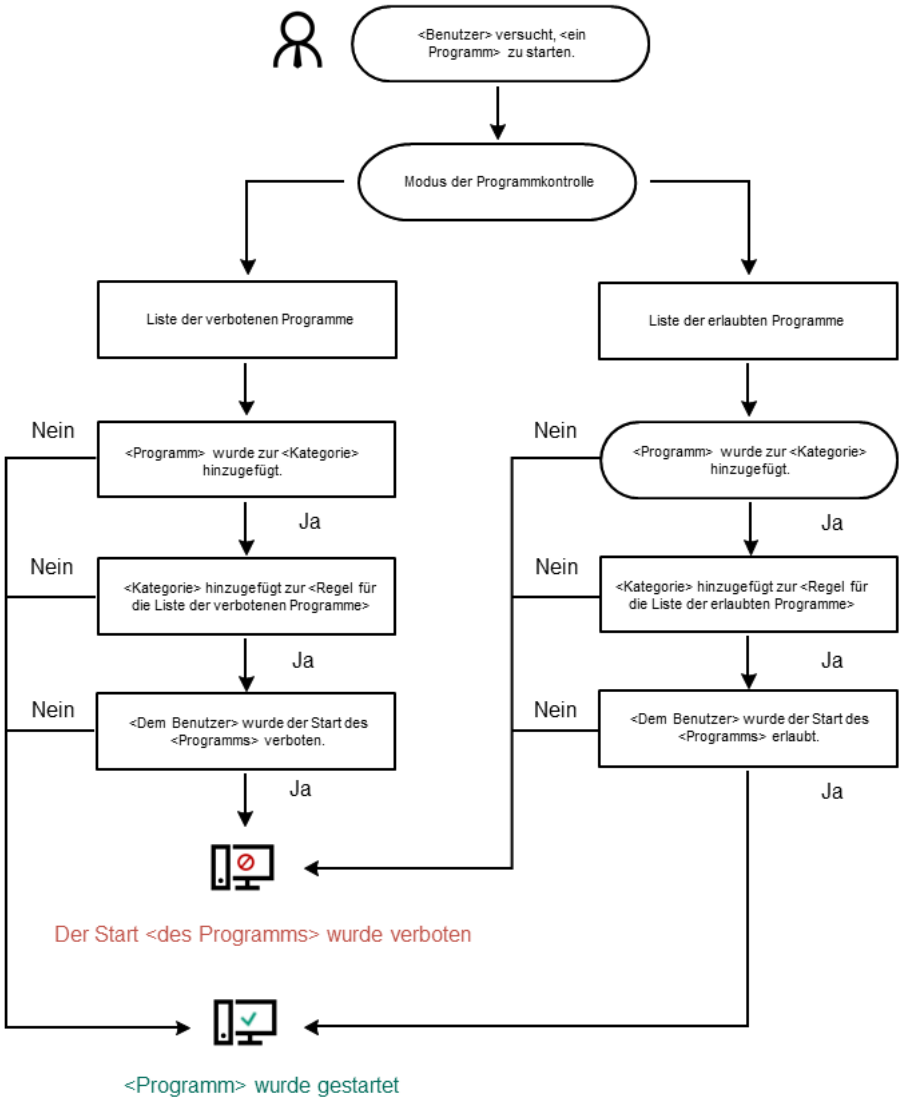
  Die Regeln der Programmkontrolle, die in der Verwaltungskonsole von Kaspersky Security Center erstellt wurden, beruhen auf den von Ihnen erstellten Programmkategorien, und nicht wie in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security auf ein- und ausschließenden Bedingungen.

- Empfang von Informationen über die Programme, die auf den Computern des lokalen Unternehmensnetzwerks installiert sind

Deshalb wird empfohlen, die Komponente „Programmkontrolle" mithilfe von Kaspersky Security Center anzupassen.

Algorithmus der „Programmkontrolle"

Kaspersky Endpoint Security verwendet einen Algorithmus, um über den Start eines Programms zu entscheiden (s. Abb. unten).



Algorithmus der „Programmkontrolle"

Einstellungen für die Komponente „Programmkontrolle"

Einstellung	Beschreibung
Testmodus	Wenn der Schalter aktiviert ist, erlaubt Kaspersky Endpoint Security den Start des Programms, das im aktuellen Modus der Programmkontrolle verboten ist, und protokolliert Informationen über den Programmstart.
Modus der „Programmkontrolle"	Sie können zwischen folgenden Varianten wählen: • **Deny-Liste**. Bei Auswahl dieser Variante erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Verbotsregeln der Programmkontrolle erfüllt sind. • **Allow-Liste**. Bei Auswahl dieser Variante verbietet die Programmkontrolle allen Benutzern den Start beliebiger Programme. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Erlaubnisregeln der Programmkontrolle erfüllt sind. Bei Auswahl des Modus **Allow-Liste** werden automatisch zwei Regeln für die Programmkontrolle erstellt:

	• **Goldene Kategorie**. • **Vertrauenswürdige Programme mit Update-Funktionen**. Automatisch erstellte Regeln können nicht geändert oder gelöscht werden. Sie können diese Regeln aktivieren oder deaktivieren.
DLL kontrollieren	Ist das Kontrollkästchen aktiviert, so kontrolliert Kaspersky Endpoint Security das Laden von DLL-Modulen, wenn Programme von Benutzern gestartet werden. Informationen über das DLL-Modul und das Programm, das dieses DLL-Modul geladen hat, werden protokolliert. Wenn die Funktion zur Kontrolle des Ladens von DLL-Modulen und Treibern aktiviert ist, vergewissern Sie sich, dass in den „Programmkontrolle"-Einstellungen entweder die Regel **Goldene Kategorie** aktiviert ist oder eine andere Regel, welche die KL-Kategorie „Vertrauenswürdige Zertifikate" enthält und das Laden von DLL-Modulen und Treibern vor dem Start von Kaspersky Endpoint Security gewährleistet. Wenn die Kontrolle von DLL-Modulen und Treibern gleichzeitig mit der Regel **Goldene Kategorie** aktiviert ist, kann es zur Instabilität des Betriebssystems kommen. Kaspersky Endpoint Security kontrolliert nur jene DLL-Module und Treiber, die geladen wurden, nachdem das Kontrollkästchen aktiviert wurde. Nach dem Aktivieren des Kontrollkästchens wird empfohlen, den Computer neu zu starten, um sicherzustellen, dass das Programm alle DLL-Module und Treiber überwacht, einschließlich derer, die vor dem Start von Kaspersky Endpoint Security geladen wurden.
Vorlagen für Nachrichten	**Nachricht zum Blockieren**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert. **Nachricht an den Administrator**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn ein Programm nach Meinung des Benutzers irrtümlich blockiert wurde.

Adaptive Kontrolle von Anomalien

Diese Komponente ist nur für Kaspersky Endpoint Security for Business Advanced und Kaspersky Total Security for Business verfügbar. Ausführliche Informationen über Kaspersky Endpoint Security for Business finden Sie auf der *Kaspersky-Website*.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Adaptive Kontrolle von Anomalien“ überwacht und blockiert Aktionen, die für Computer des Unternehmensnetzwerks untypisch sind. Zur Überwachung von untypischen Aktionen verwendet die „Adaptive Kontrolle von Anomalien“ eine Auswahl von Regeln (z. B. die Regel *Start von Windows PowerShell aus einem Office-Programm*). Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt. Sie können ein Verhalten der „Adaptiven Kontrolle von Anomalien“ für jede einzelne Regeln auswählen und beispielsweise den Start von PowerShell-Skripten erlauben, um die Lösung von Unternehmensaufgaben zu automatisieren. Kaspersky Endpoint Security aktualisiert den Regelsatz aus den Programm-Datenbanken. Die Aktualisierung des Regelsatzes muss manuell bestätigt werden.

“Adaptive Kontrolle von Anomalien“ anpassen

Die Anpassung der „Adaptiven Kontrolle von Anomalien“ umfasst folgende Schritte:

1. Training der „Adaptiven Kontrolle von Anomalien“.

   Nachdem die „Adaptive Kontrolle von Anomalien“ aktiviert ist, funktionieren die Regeln im *Lernmodus*. Im Verlauf des Trainings überwacht die „Adaptive Kontrolle von Anomalien“ die Auslösung von Regeln und sendet Auslöseereignisse an Kaspersky Security Center. Jede Regel hat eine eigene Dauer für den Lernmodus. Die Dauer des Lernmodus wird von den Kaspersky-Experten vorgegeben. Gewöhnlich dauert der Lernmodus 2 Wochen.

   Wenn eine Regel während des Trainings nie ausgelöst wurde, betrachtet die „Adaptive Kontrolle von Anomalien“ die mit dieser Regel verbundenen Aktionen als untypisch. Kaspersky Endpoint Security blockiert alle Aktionen, die mit dieser Regel zusammenhängen.

   Wenn eine Regel während des Trainings ausgelöst wurde, protokolliert Kaspersky Endpoint Security die Ereignisse im Bericht über ausgelöste Regeln und im Speicher **Auslösung von Regeln im Lernmodus**.

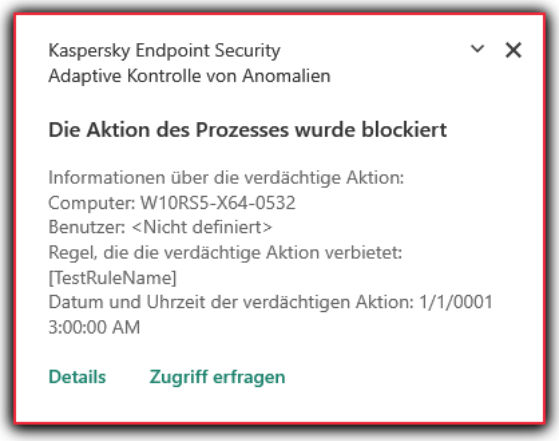
2. Analyse des Berichts über ausgelöste Regeln.

   Der Administrator analysiert den Bericht über ausgelöste Regeln oder den Inhalt des Speichers **Auslösung von Regeln im Lernmodus**. Anschließend kann der Administrator das Verhalten der „Adaptiven Kontrolle von Anomalien“ bei einer Auslösung der Regel festlegen: blockieren oder erlauben. Außerdem kann der Administrator die Regelauslösung weiterhin überwachen und die Dauer des Lernmodus für das Programm verlängern. Ergreift der Administrator keine Maßnahmen, so läuft das Programm ebenfalls im Lernmodus weiter. Die Dauer des Lernmodus beginnt von vorne.

Die „Adaptive Kontrolle von Anomalien“ wird im Echtzeitmodus angepasst. Die „Adaptive Kontrolle von Anomalien“ wird wie folgt angepasst:

- Die „Adaptive Kontrolle von Anomalien“ beginnt automatisch, jene Aktionen zu blockieren, die mit Regeln zusammenhängen, die im Lernmodus nicht ausgelöst wurden.
- Kaspersky Endpoint Security fügt neue Regeln hinzu oder löscht veraltete Regeln.
- Der Administrator passt die Verwendung der „Adaptiven Kontrolle von Anomalien“ nach der Analyse des Berichts über ausgelöste Regeln und des Inhalts des Speichers **Auslösung von Regeln im Lernmodus** an. Es wird empfohlen, den Bericht über ausgelöste Regeln und den Inhalt des Speichers **Auslösung von Regeln im Lernmodus zu überprüfen**.

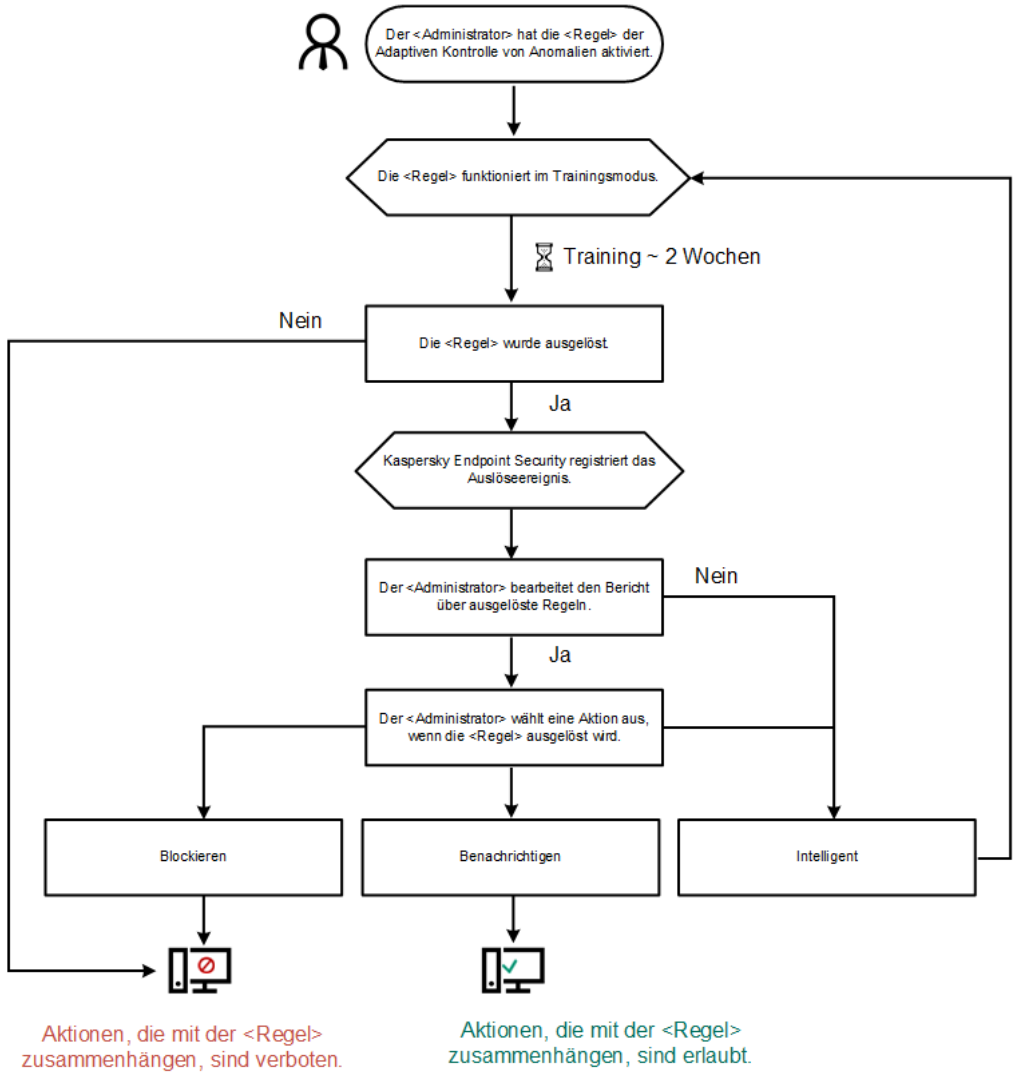
Wenn ein Schadprogramm versucht, eine Aktion auszuführen, blockiert Kaspersky Endpoint Security die Aktion und zeigt eine Benachrichtigung an (siehe Abbildung unten).



Benachrichtigung der „Adaptiven Kontrolle von Anomalien"

Algorithmus der „Adaptiven Kontrolle von Anomalien"

Um über die Ausführung einer Aktion, die mit einer Regeln verbunden ist, zu entscheiden, nutzt Kaspersky Endpoint Security den folgenden Algorithmus (siehe Abbildung unten).



Algorithmus der „Adaptiven Kontrolle von Anomalien"

Einstellungen der Komponente „Adaptive Kontrolle von Anomalien"

Einstellung	Beschreibung

Bericht zum Regelstatus *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dieser Bericht enthält Informationen zum Status der Erkennungsregeln der „Adaptiven Kontrolle von Anomalien“ (z. B. *Deaktiviert* oder *Blockieren*). Der Bericht wird für alle Administrationsgruppen erstellt.
Bericht über ausgelöste Regeln *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dieser Bericht enthält Informationen über untypische Aktionen, die mithilfe der „Adaptiven Kontrolle von Anomalien“ erkannt wurden. Der Bericht wird für alle Administrationsgruppen erstellt.
Regeln	Tabelle der Regeln der „Adaptiven Kontrolle von Anomalien“. Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für potentiell schädliche Aktivitäten erstellt.
Vorlagen	• **Nachricht zum Blockieren**. Vorlage der Nachricht an den Benutzer. Diese Nachricht wird angezeigt, wenn eine Regel der „Adaptiven Kontrolle von Anomalien“ ausgelöst wird, die eine untypische Aktion blockiert. • **Nachricht an den Administrator**. Vorlage der Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn eine Aktion nach Meinung des Benutzers irrtümlich blockiert wurde.

Endpoint Sensor

In Kaspersky Endpoint Security 11.4.0 ist die Komponente Endpoint Sensor nicht im Programm enthalten.

Sie können „Endpoint Sensor“ in Kaspersky Security Center 12 Web Console und in der „Verwaltungskonsole“ für Kaspersky Security Center verwalten. “Endpoint Sensor“ kann nicht im Programm Kaspersky Security Center Cloud Console verwaltet werden.

Endpoint Sensor dient der Interaktion mit Kaspersky Anti Targeted Attack Platform. Die Lösung *Kaspersky Anti Targeted Attack Platform* dient der rechtzeitigen Erkennung komplexer Bedrohungen. Dazu zählen beispielsweise gezielte Angriffe, hoch entwickelte hartnäckige Bedrohungen (APT, Advanced Persistent Threat) und Zero-Day-Angriffe. Kaspersky Anti Targeted Attack Platform umfasst zwei funktionale Blöcke: Kaspersky Anti Targeted Attack (im Folgenden "*KATA*") und Kaspersky Endpoint Detection and Response (im Folgenden "*KEDR*"). Sie können KEDR separat erwerben. Detaillierte Informationen über die Lösung. *finden Sie in der Hilfe zur Kaspersky Anti Targeted Attack Platform*.

Für die Verwaltung von Endpoint Sensor gelten die folgenden Besonderheiten:

- Wenn auf dem Computer das Programm Kaspersky Endpoint Security Versionen 11.0.0 – 11.3.0 installiert ist, können Sie die Einstellungen von Endpoint Sensor mithilfe einer Richtlinie anpassen. Details zum Anpassen der Einstellungen von „Endpoint Sensor“ mithilfe einer Richtlinie finden Sie in der *Hilfe zu Kaspersky Endpoint Security für die vorhergehenden Versionen*.
- Wenn auf dem Computer das Programm Kaspersky Endpoint Security Version 11.4.0 oder höher installiert ist, können die Einstellungen von Endpoint Sensor nicht mithilfe einer Richtlinie angepasst werden.

“Endpoint Sensor“ wird auf den Client-Computern installiert. Auf diesen Computern überwacht die Komponente permanent Prozesse, geöffnete Netzwerkverbindungen und veränderte Dateien. Endpoint Sensor überträgt Informationen an den KATA-Server.

Die Funktionalität der Komponente ist für die folgenden Betriebssysteme verfügbar:

- Windows 7 Service Pack 1 Home / Professional / Enterprise
- Windows 8.1.1 Professional / Enterprise
- Windows 10 RS3 Home / Professional / Education / Enterprise
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-Bit)
- Windows Server 2012 Foundation / Standard / Enterprise (64-Bit)
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-Bit)

Ausführliche Informationen über die Funktionsweise von KATA *finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform*.

Vollständige Festplattenverschlüsselung

Sie können ein Verschlüsselungsverfahren auswählen: Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung (im Folgenden auch „BitLocker“ genannt).

Kaspersky-Festplattenverschlüsselung

Nach der Verschlüsselung von Systemfestplatten und einem nachfolgenden Neustart des Computers, sind der Zugriff auf die Festplatten und das Laden des Betriebssystems erst möglich, nachdem der Benutzer sich mithilfe des Authentifizierungsagenten authentifiziert hat. Dazu ist entweder die Eingabe des Kennworts für den Token oder die Smartcard, die mit dem Computer verbunden sind, oder die Eingabe von Benutzername und Kennwort für das Authentifizierungsagenten-Benutzerkonto erforderlich, das vom Systemadministrator des lokalen Unternehmensnetzwerks mithilfe der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* erstellt wurde. Diese Konten basieren auf den Benutzerkonten von Microsoft Windows, mit denen sich die Benutzer im Betriebssystem anmelden. Sie können auch das Verfahren zur Einmalanmeldung (SSO, Single Sign-On) nutzen. Es ermöglicht eine automatische Anmeldung im Betriebssystem mit dem Benutzernamen und dem Kennwort des Authentifizierungsagenten-Benutzerkontos.

Es gibt zwei Methoden, mit denen sich der Benutzer im Authentifizierungsagenten authentifizieren kann:

- Durch Eingabe von Name und Kennwort eines Benutzerkontos für den Authentifizierungsagenten, wenn das Benutzerkonto vom Administrator des lokalen Unternehmensnetzwerks mit Mitteln von Kaspersky Security

Center erstellt wurde.

- Durch Eingabe des Kennworts für einen Token oder eine Smartcard, die mit dem Computer verbunden sind.

  Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

BitLocker-Laufwerkverschlüsselung

BitLocker ist eine integrierte Verschlüsselungstechnologie des Windows-Betriebssystems. Kaspersky Endpoint Security ermöglicht es, BitLocker mithilfe von Kaspersky Security Center zu kontrollieren und zu verwalten. BitLocker verschlüsselt ein logisches Volume. Wechseldatenträger können mithilfe von BitLocker nicht verschlüsselt werden. Details über BitLocker finden Sie in der Microsoft-Dokumentation.

Die Sicherheit beim Speichern von Zugriffsschlüsseln gewährleistet BitLocker mithilfe von Trusted Platform Module. *Trusted Platform Module (TPM)* ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Ein Trusted Platform Module wird normalerweise auf der Hauptplatine des Computers installiert und interagiert mit allen anderen Systemkomponenten über die Hardwareschnittstelle. Die Verwendung des TPM ist die sicherste Art, BitLocker-Zugriffsschlüssel zu speichern, da das TPM eine Überprüfung der Systemintegrität vor dem Systemstart ermöglicht. Auf Computern ohne TPM können Sie Laufwerke verschlüsseln. Dabei wird der Zugriffsschlüssel mit einem Kennwort verschlüsselt. BitLocker verwendet die folgenden Authentifizierungsmethoden:

- TPM.
- TPM und PIN-Code.
- Kennwort.

Nach der Laufwerkverschlüsselung erstellt BitLocker einen Master-Schlüssel. Kaspersky Endpoint Security sendet den Master-Schlüssel an Kaspersky Security Center, damit Sie den Zugriff auf das Laufwerk wiederherstellen können, beispielsweise wenn der Benutzer das Kennwort vergisst.

Wenn der Benutzer mithilfe von BitLocker selbständig ein Laufwerk verschlüsselt hat, sendet Kaspersky Endpoint Security Informationen über die Laufwerksverschlüsselung an Kaspersky Security Center. Den Master-Schlüssel sendet Kaspersky Endpoint Security dabei nicht an Kaspersky Security Center. Darum lässt sich der Zugriff auf das Laufwerk mithilfe von Kaspersky Security Center nicht wiederherstellen. Damit BitLocker mit Kaspersky Security Center ordnungsgemäß funktioniert, entschlüsseln Sie das Laufwerk und verschlüsseln Sie es erneut mithilfe der Richtlinie. Sie können das Laufwerk entweder lokal oder mithilfe der Richtlinie entschlüsseln.

Nachdem die Systemfestplatte verschlüsselt wurde, von der das Betriebssystem gestartet wird, muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach dem Authentifizierungsverfahren ermöglicht BitLocker die Anmeldung von Benutzern. BitLocker unterstützt keine Single-Sign-On-Technologie (SSO).

Wenn Sie Gruppenrichtlinien für Windows verwenden, deaktivieren Sie die BitLocker-Verwaltung in den Richtlinieneinstellungen. Es kann sein, dass die Windows-Richtlinieneinstellungen den Richtlinieneinstellungen von Kaspersky Endpoint Security widersprechen. Bei einer Laufwerksverschlüsselung könnten deshalb Fehler auftreten.

Einstellungen der Komponente „Kaspersky-Festplattenverschlüsselung"

Einstellung	Beschreibung

Verschlüsselungsmodus	**Alle Festplatten verschlüsseln**. Ist dieses Element ausgewählt und die Richtlinie wird übernommen, so verschlüsselt das Programm alle Festplatten. Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem das Programm installiert ist. **Alle Festplatten entschlüsseln**. Ist dieses Element ausgewählt und die Richtlinie wird übernommen, so entschlüsselt das Programm alle zuvor verschlüsselten Festplatten. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.
Während der Verschlüsselung automatisch Authentifizierungsagenten-Konten für Windows-Benutzer erstellen	Wenn dieses Kontrollkästchen aktiviert ist, erstellt das Programm Benutzerkonten des Authentifizierungsagenten basierend auf der Liste der Windows-Benutzerkonten auf dem Computer. Kaspersky Endpoint Security verwendet standardmäßig alle lokalen und Domänen-Benutzerkonten, mit denen sich der Benutzer in den letzten 30 Tagen am Betriebssystem angemeldet hat.
Einstellungen für das Erstellen von Benutzerkonten für den Authentifizierungsagenten	**Alle Benutzerkonten des Computers**. Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung Authentifizierungsagenten-Benutzerkonten für alle Benutzerkonten des Computers, die schon einmal aktiv waren. **Alle Domänenkonten des Computers**. Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung Authentifizierungsagenten-Benutzerkonten für alle Benutzerkonten des Computers, die zu einer Domäne gehören und schon einmal aktiv waren. **Alle lokalen Benutzerkonten des Computers**. Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung Authentifizierungsagenten-Benutzerkonten für alle lokalen Benutzerkonten des Computers, die schon einmal aktiv waren. **Lokaler Administrator**. Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung ein Benutzerkonto für den lokalen Administrator. **Manager des Computers**. Wenn das Kontrollkästchen aktiviert ist, erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung ein Authentifizierungsagenten-Benutzerkonto für jenes Benutzerkonto, das in den Active Directory-Eigenschaften als Manager angegeben ist. **Aktives Benutzerkonto**. Ist das Kontrollkästchen aktiviert ist, so erstellt Kaspersky Endpoint Security im Rahmen der Aufgabe zur vollständigen Festplattenverschlüsselung automatisch ein Authentifizierungsagenten-Benutzerkonto für das Benutzerkonto des Computers, das bei der Aufgabenausführung aktiv ist.
Bei der Anmeldung automatisch Authentifizierungsagenten-Konten für alle Benutzer dieses Computers erstellen	Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm Informationen zu Windows-Benutzerkonten auf dem Computer, bevor der Authentifizierungsagent gestartet wird. Wenn Kaspersky Endpoint Security ein Windows-Benutzerkonto erkennt, das kein Benutzerkonto des Authentifizierungsagenten besitzt, erstellt das Programm ein neues Konto

	für den Zugriff auf verschlüsselte Laufwerke. Das neue Benutzerkonto des Authentifizierungsagenten verfügt über die folgenden Standardeinstellungen: nur kennwortgeschützte Anmeldung, Kennwortänderung bei der ersten Authentifizierung. Es ist also nicht nötig, für Computer mit bereits verschlüsselten Laufwerken Benutzerkonten des Authentifizierungsagenten manuell mithilfe der Aufgabe *Benutzerkonten des Authentifizierungsagenten verwalten* hinzuzufügen.
Benutzernamen speichern, der im Authentifizierungsagenten eingegeben wurde	Wenn das Kontrollkästchen aktiviert ist, speichert das Programm den Namen des Authentifizierungsagenten-Kontos. Wenn im Authentifizierungsagenten das nächste Mal eine Authentifizierung mit demselben Benutzerkonto erfolgt, muss der Benutzername nicht eingegeben werden.
Nur belegten Speicherplatz verschlüsseln	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
“Legacy USB Support“ verwenden	Das Kontrollkästchen aktiviert/deaktiviert die Funktion „Legacy USB Support“. *Legacy USB Support* **ist eine** BIOS-/UEFI-Funktion, die es ermöglicht, USB-Geräte (z. B. ein Token) zu verwenden, wenn der Computer gestartet wird und das Betriebssystem noch nicht gestartet wurde (BIOS-Modus). Nach dem Start des Betriebssystems beeinflusst die Funktion „Legacy USB Support“ die Unterstützung von USB-Geräten nicht mehr. Ist das Kontrollkästchen aktiviert, so wird die Unterstützung von USB-Geräten zu Beginn des Startvorgangs des Computers aktiviert.

	Wenn die Funktion „Legacy USB Support“ aktiviert ist, unterstützt der Authentifizierungsagent im BIOS-Modus die Verwendung von USB-Tokens nicht. Die Funktion sollte nur beim Auftreten von Hardware-Kompatibilitätsproblemen verwendet werden und ausschließlich für jene Computer aktiviert werden, auf welchen das Problem aufgetreten ist.
Einstellungen für Kennwörter	Einstellungen für die Stärke des Kennworts für ein Authentifizierungsagenten-Benutzerkonto Sie können auch die Verwendung des Verfahrens zur Einmalanmeldung (SSO) aktivieren. Die Technologie zur Einmalanmeldung erlaubt es, die gleichen Anmeldedaten für den Zugriff auf verschlüsselte Festplatten und für die Anmeldung am Betriebssystem zu verwenden. Ist das Kontrollkästchen aktiviert, so müssen für den Zugriff auf verschlüsselte Festplatten und für die nachfolgende automatische Anmeldung am Betriebssystem die Anmeldedaten für den Zugriff auf die verschlüsselten Datenträger eingegeben werden. Ist das Kontrollkästchen deaktiviert, so müssen für den Zugriff auf verschlüsselte Festplatten und für die nachfolgende Anmeldung am Betriebssystem die Anmeldedaten für den Zugriff auf verschlüsselte Festplatten und die Anmeldedaten des Benutzers im Betriebssystem separat eingegeben werden.
Hilfetexte	**Authentifizierung**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn die Anmeldedaten eingegeben werden. **Kennwort ändern**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn das Kennwort für das Authentifizierungsagenten-Benutzerkonto geändert wird. **Kennwort wiederherstellen**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn das Kennwort für das Authentifizierungsagenten-Benutzerkonto wiederhergestellt wird.

Einstellungen der Komponente „BitLocker-Laufwerkverschlüsselung“

Einstellung	Beschreibung
Verschlüsselungsmodus	**Alle Festplatten verschlüsseln**. Ist dieses Element ausgewählt und die Richtlinie wird übernommen, so verschlüsselt das Programm alle Festplatten. Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem das Programm installiert ist. **Alle Festplatten entschlüsseln**. Ist dieses Element ausgewählt und die Richtlinie wird übernommen, so entschlüsselt das Programm alle zuvor verschlüsselten Festplatten. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.
Verwendung der BitLocker-Authentifizierung aktivieren,	Das Kontrollkästchen aktiviert/deaktiviert die Verwendung der Authentifizierung, bei der eine Preboot-Tastatureingabe erforderlich ist,

die Preboot-Tastatureingaben auf Tablets erfordert	selbst dann, wenn die Plattform keine Option zur Preboot-Eingabe bietet (beispielsweise bei berührungsempfindlichen Tastaturen auf Tablets). Das Touchpad von Tablets ist in der Preboot-Umgebung nicht verfügbar. Um die BitLocker-Authentifizierung auf Tablets auszuführen, muss der Benutzer beispielsweise eine USB-Tastatur anschließen. Ist das Kontrollkästchen aktiviert, so wird die Verwendung der Authentifizierung erlaubt, wenn sie eine Preboot-Tastatureingabe erfordert. Es wird empfohlen, diese Einstellung nur für Geräte zu verwenden, die während des Preboot-Vorgangs außer berührungsempfindlichen Tastaturen auch Alternativen für die Dateneingabe bieten, wie beispielsweise eine USB-Tastatur. Wenn das Kontrollkästchen deaktiviert ist, ist die BitLocker-Laufwerkverschlüsselung auf Tablets nicht möglich.
Hardwareverschlüsselung verwenden	Ist das Kontrollkästchen aktiviert, so verwendet das Programm die Hardwareverschlüsselung. Dadurch wird erlaubt, die Verschlüsselung zu beschleunigen und die Auslastung der Computerressourcen zu reduzieren.
Nur belegten Speicherplatz verschlüsseln (Windows 8 und höhere Versionen)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Dieses Kontrollkästchen ist standardmäßig deaktiviert.
Authentifizierungseinstellungen	**Kennwort verwenden (Windows 8 und höhere Versionen)**

Bei Auswahl dieser Variante fragt Kaspersky Endpoint Security beim Benutzer das Kennwort ab, wenn auf das verschlüsselte Laufwerk zugegriffen wird.

Diese Variante für die Aktion kann gewählt werden, wenn das Trusted Platform Module (TPM) nicht verwendet wird.

Trusted Platform Module (TPM) verwenden

Bei Auswahl dieser Variante verwendet BitLocker das Trusted Platform Module (TPM).

Trusted Platform Module (TPM) ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten.

Für Computer mit den Betriebssystemen Windows 7 und Windows Server 2008 R2 ist nur die Verschlüsselung unter Verwendung eines TPM-Moduls verfügbar. Wenn kein TPM-Modul installiert ist, ist die BitLocker-Verschlüsselung nicht möglich. Die Verwendung eines Kennworts wird auf diesen Computern nicht unterstützt.

Ein Gerät, das mit Trusted Platform Module ausgerüstet ist, kann Chiffrierschlüssel erstellen, die nur seiner Hilfe entschlüsselt werden können. Das Trusted Platform Module verschlüsselt Chiffrierschlüssel mit einem eigenen Storage Root Key. Der Storage Root Key wird im Trusted Platform Module aufbewahrt. Dadurch wird für die Chiffrierschlüssel ein zusätzlicher Schutz vor Angriffsversuchen gewährleistet.

Diese Aktion ist standardmäßig ausgewählt.

Sie können eine zusätzliche Schutzebene für den Zugriff auf den Chiffrierschlüssel einrichten und den Schlüssel mit einem Kennwort oder einer PIN verschlüsseln:

- **PIN für TPM verwenden**. Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer einen PIN-Code verwenden, um auf einen Chiffrierschlüssel zuzugreifen, der im Trusted Platform Module (TPM) aufbewahrt wird.
  Wenn das Kontrollkästchen deaktiviert ist, ist es dem Benutzer verboten, einen PIN-Code zu verwenden. Um Zugriff auf den Chiffrierschlüssel zu erhalten, verwendet der Benutzer ein Kennwort. Sie können dem Benutzer erlauben, eine erweiterte PIN zu verwenden. Eine *erweiterte PIN* ermöglicht neben der Verwendung numerischer Zeichen auch lateinische Groß- und Kleinbuchstaben, Sonderzeichen und Leerzeichen.

- **Trusted Platform Module (TPM) verwenden; falls nicht verfügbar, Kennwort verwenden**. Ist das Kontrollkästchen aktiviert, so kann der Benutzer beim Fehlen des Trusted Platform Module (TPM) mithilfe des Kennworts Zugriff auf die Chiffrierschlüssel erhalten.

  Wenn das Kontrollkästchen deaktiviert ist und das TPM-Modus nicht verfügbar ist, wird die vollständige Festplattenverschlüsselung nicht gestartet.

Verschlüsselung von Dateien

Sie können folgende Listen anlegen: Listen mit Dateien nach Erweiterung oder Erweiterungsgruppen, und Listen mit Ordnern, die sich auf lokalen Laufwerken des Computers befinden. Außerdem können Sie Verschlüsselungsregeln für Dateien definieren, die von bestimmten Programmen erstellt werden. Nachdem die Richtlinie übernommen wurde, verschlüsselt und entschlüsselt Kaspersky Endpoint Security die folgenden Dateien:

- Dateien, die einzeln zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
- Dateien, die in Ordnern gespeichert sind, welche zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
- Dateien, die von bestimmten Programmen erstellt werden

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Kaspersky Endpoint Security verschlüsselt/entschlüsselt die Standardordner nur für die lokalen Benutzerprofile (local user profiles) des Betriebssystems. Kaspersky Endpoint Security verschlüsselt und entschlüsselt die Standardordner nicht für Roaming-Benutzerprofile (roaming user profiles), verbindliche Benutzerprofile (mandatory user profiles), temporäre Benutzerprofile (temporary user profiles) und Ordnerumleitung.
- Für Dateien, deren Veränderung die Funktionsfähigkeit des Betriebssystems und der installierten Programme beeinträchtigen kann, führt Kaspersky Endpoint Security keine Verschlüsselung durch. Zur Liste der Verschlüsselungsausnahmen gehören beispielsweise folgende Dateien und Ordner mit allen untergeordneten Ordnern:
  - %WINDIR%
  - %PROGRAMFILES% und %PROGRAMFILES(X86)%
  - Dateien der Systemregistrierung von Windows

  Die Liste mit Ausnahmen von der Verschlüsselung kann nicht angezeigt oder geändert werden. Dateien und Ordner aus der Liste mit den Verschlüsselungsausnahmen können zur Verschlüsselungsliste hinzugefügt werden; sie werden jedoch bei der Ausführung der Dateiverschlüsselung nicht verschlüsselt.

Einstellungen der Komponente „Dateien verschlüsseln"

Einstellung	Beschreibung
Verwaltung der Verschlüsselung	**Nicht verändern**. Bei Auswahl dieses Elements belässt Kaspersky Endpoint Security die Dateien und Ordner im gleichen Zustand, d.h. sie werden nicht verschlüsselt oder entschlüsselt. **Nach den Regeln verschlüsseln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor: Dateien und Ordner werden gemäß den Verschlüsselungsregel verschlüsselt, Dateien und Ordner werden gemäß den Entschlüsselungsregel entschlüsselt, und der Zugriff von Programmen auf verschlüsselte Dateien wird nach den Regeln für Programme geregelt.

	Alle entschlüsseln. Bei Auswahl dieses Elements entschlüsselt Kaspersky Endpoint Security alle verschlüsselten Dateien und Ordner.
Verschlüsselungsregeln	Auf dieser Registerkarte werden die Regeln für die Verschlüsselung der Dateien angezeigt, die auf lokalen Laufwerken gespeichert sind. Sie können Dateien wie folgt hinzufügen: • **Standardordner**. Kaspersky Endpoint Security erlaubt es, die folgenden Bereiche hinzuzufügen: **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner. **Favoriten**. Dateien im Standardordner *Favoriten* des Betriebssystems, sowie untergeordnete Ordner. **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner. **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Sicherungskopien von Dokumenten. **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB). • **Ordner**. Sie können einen Ordnerpfad eingeben. Beachten Sie folgende Regeln, wenn Sie einen Ordnerpfad hinzufügen: Verwenden Sie eine Umgebungsvariable (z. B. `%FOLDER%\UserFolder\`). Eine Umgebungsvariable kann nur ein Mal und nur am Anfang des Pfads verwendet werden. Verwenden Sie keine relativen Pfade. Sie können einen Satz verwenden `\..\` (z. B. `C:\Users\..\UserFolder\`). Der Satz `\..\` bedeutet einen Wechsel zum übergeordneten Ordner. Verwenden Sie nicht die Zeichen `*` und `?`. Verwenden Sie keine UNC-Pfade. Verwenden Sie `;` oder `,` als Trennzeichen. • **Dateien nach Erweiterung**. Sie können aus der Liste eine Gruppe mit Erweiterungen auswählen, z. B. die Erweiterungsgruppe *Archive*. Außerdem können Sie eine Dateierweiterung manuell hinzufügen.
Entschlüsselungsregeln	Auf dieser Registerkarte werden die Entschlüsselungsregeln für Dateien angezeigt, die auf lokalen Laufwerken gespeichert sind.
Regeln für Programme	Auf dieser Registerkarte wird eine Tabelle mit Zugriffsregeln für Programme auf verschlüsselte Dateien und mit Verschlüsselungsregeln für Dateien angezeigt. Die Regeln beziehen sich auf Dateien, die von bestimmten Programmen erstellt und geändert wurden.
Kennworteinstellungen für verschlüsselte Archive	Einstellungen für die Kennwortstärke, die beim Erstellen verschlüsselter Archive gelten sollen.

Wechseldatenträger verschlüsseln

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Kaspersky Endpoint Security unterstützt die Dateiverschlüsselung in FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselung dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus „Nur Lesen“ fest.

Um die Daten auf Wechseldatenträgern zu schützen, können Sie folgende Verschlüsselungsmethoden verwenden:

- Vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE).

  Verschlüsselung des gesamten Wechseldatenträgers, einschließlich des Dateisystems.

  Es ist nicht möglich, außerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen. Außerdem ist es nicht möglich, innerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen, wenn der Computer nicht mit Kaspersky Security Center (“Gast-Computer“) verbunden ist.

- Verschlüsselung von Dateien (File Level Encryption, FLE).

  Nur Dateien auf dem Wechseldatenträger verschlüsseln. Dabei wird das Dateisystem nicht verändert.

  Die Verschlüsselung von Dateien auf Wechseldatenträgern ermöglicht es, auch außerhalb des Unternehmensnetzwerks auf die Daten zuzugreifen. Dazu dient der *portable Modus*.

Bei der Verschlüsselung erstellt Kaspersky Endpoint Security einen Master-Schlüssel. Kaspersky Endpoint Security speichert den Master-Schlüssel in den folgenden Speichern:

- Kaspersky Security Center.
- Benutzercomputer.

  Der Master-Schlüssel wird mit einem Geheimschlüssel des Benutzers verschlüsselt.
- Wechseldatenträger.

  Der Master-Schlüssel wird mit einem offenen Schlüssel von Kaspersky Security Center verschlüsselt.

Nach der Verschlüsselung sind die Daten auf dem Wechseldatenträger innerhalb des Unternehmensnetzwerks verfügbar, als würde ein gewöhnlicher unverschlüsselter Wechseldatenträger verwendet.

Zugriffserteilung auf verschlüsselte Daten

Wenn eine Wechseldatenträger mit verschlüsselten Daten verbunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

1. Es wird überprüft, ob in der lokalen Datenverwaltung auf dem Benutzercomputer ein Master-Schlüssel vorhanden ist.

   Wenn ein Master-Schlüssel gefunden wird, erhält der Benutzer Zugriff auf die Daten des Wechseldatenträgers.

   Wenn kein Master-Schlüssel gefunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

a. Es wird eine Anfrage an Kaspersky Security Center gesendet.

   Daraufhin sendet Kaspersky Security Center eine Antwort mit einem Master-Schlüssel.

b. Kaspersky Endpoint Security speichert den Master-Schlüssel in der lokalen Datenverwaltung auf dem Benutzercomputer, um ihn künftig für den verschlüsselten Wechseldatenträger zu verwenden.

2. Die Daten werden entschlüsselt.

Besonderheiten bei der Verschlüsselung von Wechseldatenträgern

Für die Verschlüsselung von Wechseldatenträgern gelten die folgenden Besonderheiten:

- Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Gruppe von verwalteten Computern erstellt. Deshalb ist das Ergebnis, das durch das Übernehmen der Richtlinie für Kaspersky Security Center mit angepasster Verschlüsselung/Entschlüsselung von Wechseldatenträgern erreicht wird, davon abhängig, mit welchen Computern ein Wechseldatenträger verbunden ist.

- Für Dateien mit dem Zugriffsstatus „nur Lesen“, die auf Wechseldatenträgern gespeichert sind, führt Kaspersky Endpoint Security keine Dateiverschlüsselung/-entschlüsselung durch.

- Als Wechseldatenträger werden folgende Gerätetypen unterstützt:

  - Datenträger, die über eine USB-Schnittstelle verbunden werden

  - Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

  - SSD-Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

Einstellungen der Komponente „Wechseldatenträger verschlüsseln“

Einstellung	Beschreibung
Verwaltung der Verschlüsselung	**Gesamten Wechseldatenträger verschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Wechseldatenträger werden sektorweise verschlüsselt, einschließlich der Dateisysteme der Wechseldatenträger. **Alle Dateien verschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Alle Dateien, die auf Wechseldatenträgern gespeichert sind, werden verschlüsselt. Bereits verschlüsselte Dateien werden von Kaspersky Endpoint Security nicht erneut verschlüsselt. Der Inhalt des Dateisystems von Wechseldatenträgern sowie die Namen verschlüsselter Dateien und die Ordnerstruktur bleiben verfügbar und werden nicht verschlüsselt.

	Nur neue Dateien verschlüsseln. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Auf Wechseldatenträgern werden nur jene Dateien verschlüsselt, die hinzugefügt oder geändert wurden, nachdem die Richtlinie für Kaspersky Security Center zum letzten Mal übernommen wurde. Dieser Verschlüsselungsmodus kann praktisch sein, wenn der Benutzer einen Wechseldatenträger sowohl privat als auch geschäftlich nutzt. Der Verschlüsselungsmodus erlaubt es, alle alten Dateien unverändert zu lassen und nur jene Dateien zu verschlüsseln, die der Benutzer auf einem PC erstellt, auf dem Kaspersky Endpoint Security installiert ist und auf dem die Verschlüsselungsfunktion zur Verfügung steht. Dadurch ist ein Zugriff auf persönliche Dateien immer möglich, unabhängig davon, ob das Programm Kaspersky Endpoint Security auf dem Computer installiert ist und ob die Verschlüsselungsfunktion verfügbar ist oder nicht. **Gesamten Wechseldatenträger entschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Es werden alle verschlüsselten Dateien entschlüsselt, die auf Wechseldatenträgern gespeichert sind, sowie die Dateisysteme der Wechseldatenträger, falls diese verschlüsselt waren. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.
Portabler Modus	Dieses Kontrollkästchen aktiviert/deaktiviert die Erstellung eines Wechseldatenträgers, der es erlaubt, mit den Dateien, die auf diesem Wechseldatenträger gespeichert sind, auf Computern außerhalb des Unternehmensnetzwerks zu arbeiten. Wenn dieses Kontrollkästchen aktiviert ist und die Richtlinie übernommen wird, fragt Kaspersky Endpoint Security den Benutzer nach dem Kennwort, bevor mit der Verschlüsselung von Dateien auf einem Wechseldatenträger begonnen wird. Dieses Kennwort ist erforderlich, um auf Computern außerhalb des Unternehmensnetzwerks Zugriff auf verschlüsselte Dateien auf dem Wechseldatenträger zu erhalten. Sie können die Kennwortkomplexität anpassen. Der portable Modus ist für die Modi **Alle Dateien verschlüsseln** und **Nur neue Dateien verschlüsseln** verfügbar.
Nur belegten Speicherplatz verschlüsseln	Das Kontrollkästchen aktiviert/deaktiviert einen Verschlüsselungsmodus, bei dem nur die belegten Sektoren eines Laufwerks verschlüsselt werden. Dieser Modus wird für neuen Laufwerke empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Ist das Kontrollkästchen aktiviert, so wird nur der Teil eines Laufwerks verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist dieses Kontrollkästchen deaktiviert, so wird das gesamte Laufwerk verschlüsselt. Dabei werden auch die Bestandteile von bereits gelöschten oder geänderten Dateien verschlüsselt. Die Funktion, bei der nur belegter Speicherplatz verschlüsselt wird, ist nur für den Modus **Gesamten Wechseldatenträger verschlüsseln** verfügbar.

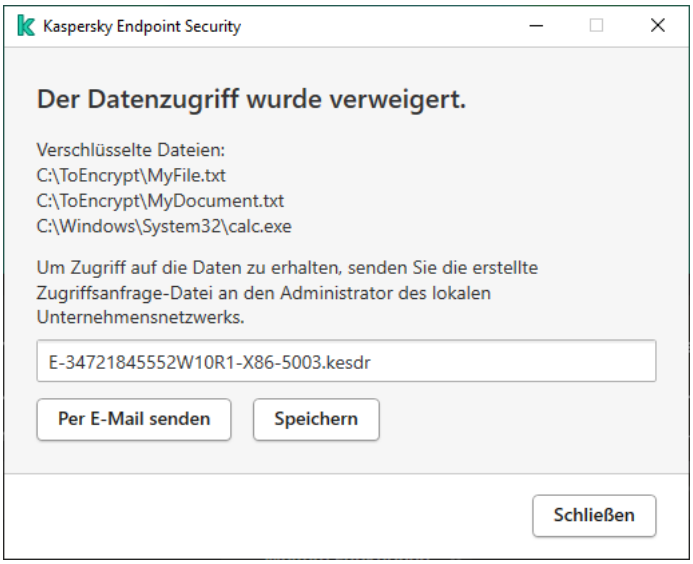
	Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln** nach dem Start der Verschlüsselung aktiviert/deaktiviert wird, wird diese Einstellung nicht beeinflusst. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden.

Verschlüsselungsregeln für die ausgewählten Geräte	Tabelle der Geräte, für die individuelle Verschlüsselungsregeln festgelegt sind. Es gibt folgende Möglichkeiten, um Verschlüsselungsregeln für bestimmte Wechseldatenträger zu erstellen:
	• Hinzufügen eines Wechseldatenträgers aus der Liste der vertrauenswürdigen Geräte der „Gerätekontrolle“.
	• Manuelles Hinzufügen eines Wechseldatenträgers:
	  • nach Geräte-ID (Hardware ID, HWID)
	  • nach dem Gerätemodell: Hersteller-ID (Vendor ID, VID) und Produkt-ID (Product ID, PID)

Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben	Ist das Kontrollkästchen aktiviert, so verschlüsselt Kaspersky Endpoint Security die Wechseldatenträger auch dann, wenn keine Verbindung zu Kaspersky Security Center besteht. Die Daten, die zur Entschlüsselung von Wechseldatenträgern erforderlich sind, werden dabei auf der Festplatte des Computers gespeichert, mit dem der Wechseldatenträger verbunden ist, und werden nicht an Kaspersky Security Center übertragen. Wenn dieses Kontrollkästchen deaktiviert ist, verschlüsselt Kaspersky Endpoint Security Wechseldatenträger nicht, wenn keine Verbindung zu Kaspersky Security Center besteht.
Kennworteinstellungen für den portablen Modus	Einstellungen für die Stärke des Kennworts für den portablen Dateimanager.

Vorlagen (Datenverschlüsselung)

Kaspersky Endpoint Security kann nach der Datenverschlüsselung den Datenzugriff verbieten, beispielsweise wenn sich die Unternehmensinfrastruktur oder der Kaspersky Security Center Administrationsserver geändert hat. Wenn der Benutzer keinen Zugriff auf verschlüsselte Daten hat, kann er beim Administrator den Datenzugriff anfordern. Dazu muss der Benutzer eine Zugriffsanfrage-Datei übermitteln. Dann muss der Benutzer die Antwortdatei, die er vom Administrator erhält, in Kaspersky Endpoint Security laden. In Kaspersky Endpoint Security ist es möglich, den Administrator per E-Mail um Datenzugriff zu bitten (s. Abb. unten).



Anfrage für den Zugriff auf verschlüsselte Daten

Es gibt eine Vorlage für die Nachricht, die über fehlenden Zugriff auf verschlüsselte Daten benachrichtigt. Um es dem Benutzer leichter zu machen, können Sie die folgenden Felder ausfüllen:

- **An**. Geben Sie die E-Mail-Adresse der Administratorengruppe ein, die über Rechte für die Datenverschlüsselungsfunktion verfügt.
- **Betreff**. Geben Sie einen Betreff der Nachricht mit einer Zugriffsanfrage für verschlüsselte Dateien ein. Sie können beispielsweise Tags hinzufügen, um diese Nachrichten zu filtern.
- **Nachricht**. Ändern Sie bei Bedarf den Nachrichteninhalt. Sie können Variablen verwenden, um die erforderlichen Daten zu erhalten (z. B. die Variable `%USER_NAME%`).

Ausnahmen

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt.

Die vertrauenswürdige Zone wird manuell vom Systemadministrator angelegt. Berücksichtigt werden dabei die Besonderheiten von Objekten, die für die Arbeit erforderlich sind, sowie die Programme, die auf dem Computer installiert sind. Die Aufnahme von Objekten und Programmen in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Endpoint Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt oder Programm unschädlich ist. Ein Administrator kann einem Benutzer auch erlauben, seine eigene lokale vertrauenswürdige Zone für einen bestimmten Computer zu erstellen. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen.

Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme.

Die Untersuchungsausnahmen ermöglichen es, mit legalen Programmen zu arbeiten, die von Angreifern für eine Beschädigung des Computers oder der Benutzerdaten verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Angreifern verwendet werden. Nähere Informationen zu legalen Programmen, die von Angreifern missbraucht werden können, um den Computer oder die Daten des Anwenders zu beschädigen, erhalten Sie auf der Website der Viren-Enzyklopädie von Kaspersky.

Derartige Programme können bei der Ausführung von Kaspersky Endpoint Security gesperrt werden. Sie können Untersuchungsausnahmen anpassen, um eine Sperrung von notwendigen Programmen zu verhindern. Dazu muss der vertrauenswürdigen Zone der Name oder eine Namensmaske hinzugefügt werden, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht. Es kann beispielsweise sein, dass Sie häufig mit dem Programm Radmin, zur Remote-Administration von Computern. Eine solche Programmaktivität wird von Kaspersky Endpoint Security als schädlich eingestuft und kann blockiert werden. Um zu verhindern, dass ein Programm gesperrt wird, muss eine Untersuchungsausnahme erstellt werden. In dieser Ausnahme wird ein Name oder eine Namensmaske angegeben, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht.

Ein auf Ihrem Computer installiertes Programm, das Informationen sammelt und zur Verarbeitung weiterleitet, kann von Kaspersky Endpoint Security als schädlich eingestuft werden. Um dies zu vermeiden, können Sie das Programm von der Untersuchung ausschließen. Dazu können Sie Kaspersky Endpoint Security entsprechend anpassen, wie in dieser Dokumentation beschrieben.

Untersuchungsausnahmen können von folgenden Komponenten und Programmaufgaben verwendet werden, die vom Systemadministrator erstellt wurden:

- Verhaltensanalyse.
- Exploit-Prävention.
- Programm-Überwachung.
- Schutz vor bedrohlichen Dateien.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- Untersuchungsaufgaben.

Liste der vertrauenswürdigen Programme

Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Endpoint Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme sowie den von ihnen erzeugten Netzwerkverkehr. Ein Programm, das zur Liste der vertrauenswürdigen Programme hinzugefügt wurde, wird von Kaspersky Endpoint Security allerdings aus der Untersuchung ausgeschlossen.

Wenn Sie beispielsweise die Objekte, die von dem Microsoft-Windows-Programm Editor verwendet werden, für ungefährlich und eine Untersuchung dieser Objekte für nicht erforderlich halten, so vertrauen Sie diesem Programm und sollten das Programm Editor zur Liste der vertrauenswürdigen Programme hinzufügen. Beim Untersuchen werden dann Objekte übersprungen, die von diesem Programm verwendet werden.

Außerdem können spezielle Aktionen, die von Kaspersky Endpoint Security als schädlich klassifiziert werden, im Rahmen bestimmter Programme ungefährlich sein. So ist das Abfangen eines Textes, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (z. B. Punto Switcher) ein normaler Vorgang. Es wird empfohlen, solche Programme in die Liste der vertrauenswürdigen Programme aufzunehmen, um ihre speziellen Funktionen zu berücksichtigen und sie von der Aktivitätskontrolle auszuschließen.

Wenn vertrauenswürdige Programme von der Untersuchung ausgeschlossen werden, lassen sich Kompatibilitätsprobleme von Kaspersky Endpoint Security mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Endpoint Security und durch ein anderes Antiviren-Programm). Außerdem wird dadurch die Leistung des Computers erhöht, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms werden jedoch weiterhin auf Viren und andere Schadprogramme untersucht. Verwenden Sie Untersuchungsausnahmen, um ein Programm vollständig aus der Untersuchung durch Kaspersky Endpoint Security auszuschließen.

Einstellungen für Ausnahmen

Einstellung	Beschreibung
Typen der zu erkennenden Objekte	Kaspersky Endpoint Security sucht unabhängig von den aktuellen Einstellungen stets na Viren, Würmern und Trojanern und blockiert diese. Diese Programme können dem Comp erheblichen Schaden zufügen. • Viren, Würmer

Unterkategorie: Viren und Würmer (Viruses_and_Worms)

Bedrohungsstufe: hoch

Klassische Viren und Würmer führen auf einem Computer Aktionen aus, die nicht vom Benutzer erlaubt wurden. Sie können sich selbst kopieren, wobei die Kopien ebenfalls zur Reproduktion fähig sind.

Klassischer Virus

Nachdem ein klassischer Virus in ein System eingedrungen ist, infiziert er eine Date aktiviert sich darin, führt seine schädlichen Aktionen aus und fügt anderen Dateier Kopien von sich hinzu.

Ein klassischer Virus vermehrt sich nur auf lokalen Computerressourcen und kann nicht selbständig in andere Rechner eindringen. Er kann nur auf andere Computer gelangen, wenn er seine Kopie einer Datei hinzufügt, die in einem gemeinsamen Ordner oder auf einer eingelegten CD gespeichert wird, oder wenn der Benutzer eine E-Mail-Nachricht verschickt, an welche die infizierte Datei angehängt ist.

Der Code eines klassischen Virus kann in unterschiedliche Computerbereiche, in d Betriebssystem oder in Programme eindringen. Abhängig vom Milieu werden *Dateiviren*, *Bootviren*, *Skriptviren* und *Makroviren* unterschieden.

Viren verwenden unterschiedliche Methoden, um Dateien zu infizieren. *Überschreibende Viren* (Overwriting) schreiben ihren Code anstelle des Codes ein infizierten Datei und zerstören deren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht repariert werden. *Parasitäre Viren* (Parasitic) verändern Datei wobei diese vollständig oder teilweise funktionsfähig bleiben. *Companion-Viren* (Companion) verändern Dateien nicht, sondern legen Zwillingsdateien an. Beim Öffnen einer infizierten Datei wird ihr Zwilling gestartet, der ein Virus ist. Außerdem gibt es noch folgende Virentypen: *Linkviren* (Link), Viren, *die Objektmodule* (OBJ), *Compiler-Bibliotheken* (LIB) oder *den Quelltext von Programmen* infizieren, u.a.

Wurm

Genau wie bei einem klassischen Virus aktiviert sich der Code eines Wurms nach dem Eindringen in ein System selbst und führt seine schädlichen Aktionen aus. Die Bezeichnung Wurm geht darauf zurück, dass er wie ein Wurm von Computer zu Computer „kriechen“ und seine Kopien ohne Erlaubnis des Benutzers über verschiedene Datenkanäle verbreiten kann.

Würmer werden grundsätzlich nach der Art ihrer Verbreitung unterschieden. Die folgende Tabelle klassifiziert die Wurmtypen nach der Verbreitungsmethode.

Verbreitungsmethoden von Würmern

Typ	Name	Beschreibung
Email-Worm	Email-Worm	Sie verbreiten sich über E-Mails.

		Eine infizierte E-Mail-Nachricht enthält eine angehängte Datei mit einer Wurmkopie oder einem Link zu einer solchen Datei, die sich auf einer gehackten oder speziell erstellten Website befindet. Wenn Sie die angehängte Datei öffnen, wird der Wurm aktiviert. Wenn Sie auf den Link klicken, die Datei herunterladen und dann öffnen, beginnt der Wurm auch mit seinen bösartigen Aktionen. Danach verbreitet er seine Kopien. Dazu sucht er andere E-Mail-Adressen und schickt infizierte Nachrichten an diese.
IM-Worm	SMTP-Clients	Sie verbreiten sich über IM-Clients. Ein IM-Wurm verschickt in der Regel Nachrichten mit einem Link, der zu einer Website mit seiner Kopie führt, an die Adressen der Kontaktliste. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats. Dies sind Chat-Systeme, mit denen über das Internet in Echtzeit Gespräche mit mehreren Teilnehmern möglich sind. Ein solcher Wurm veröffentlicht im Internet-Chat eine Datei mit seiner Kopie oder einem Link zu einer Datei. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
Net-Worm	Netzwürmer (Würmer für Computernetzwerke)	Sie verbreiten sich über Computernetzwerke. Im Unterschied zu anderen Wurmtypen verbreitet sich ein Netzwurm ohne Zutun des Benutzers. Er sucht im lokalen Netzwerk nach Computern, auf denen Programme laufen, die Schwachstellen aufweisen. Zu diesem Zweck schickt er ein spezielles Netzwerkpaket (Exploit), das den Wurmcode oder einen Teil davon enthält. Befindet sich ein „verwundbarer“ Computer im Netzwerk, nimmt er das Netzwerkpaket an. Nachdem der Wurm vollständig in den Computer eingedrungen ist, aktiviert er sich.
P2P-Worm	Würmer für Dateitausch-Netzwerke	Sie verbreiten sich über Peer-to-Peer-Netze Um in ein P2P-Netz einzudringen, kopiert sich der Wurm in einen Ordner, der zum Dateiaustausch verwendet wird und sich gewöhnlich auf einem PC befindet. Das P2P-Netz zeigt Informationen über diese Datei an. Ein Benutzer kann die infizierte Datei wie andere angebotene Dateien im Netzwerk „finden“, herunterladen und öffnen.

		Komplexere Würmer imitieren das Netzwerkprotokoll eines konkreten P2P-Netzes: Sie antworten positiv auf Suchanfragen und bieten ihre Kopien zum Download an.
Wurm	Sonstige Würmer	Zu den sonstigen Netzwürmern zählen: • Würmer, die ihre Kopien in Netzwerkressourcen verbreiten. Unter Verwendung von Betriebssystemfunktionen durchsuchen sie verfügbare Netzwerkordner, bauen Verbindungen zu Computern im globalen Netzwerk auf und versuchen, umfassenden Zugriff auf ihre Laufwerke zu erhalten. Im Unterschied zu den oben beschriebenen Wurmarten verbreiten sich die sonstigen Würmer nicht selbständig weiter, sondern nur, wenn der Benutzer eine Datei mit einer Wurmkopie öffnet. • Würmer, die nicht zu den in dieser Tabelle beschriebenen Verbreitungsmethoden gehören (z. B. Würmer, die sich über Mobiltelefone weiterverbreiten).

- Trojanische Programme

Subkategorie: trojanische Programme (Trojan_programs)

Bedrohungsstufe: hoch

Im Gegensatz zu Würmern und Viren erstellen trojanische Programme keine Kopier von sich. Sie dringen z. B. über E-Mails oder über den Browser in den Computer ein wenn der Benutzer eine infizierte Webseite besucht. Trojanische Programme werd unter Beteiligung des Benutzers gestartet. Unmittelbar nach ihrem Start beginnen sie mit ihren schädlichen Aktionen.

Jeder Trojaner-Typ zeigt ein individuelles Verhalten auf dem infizierten Computer. Die Hauptfunktionen von trojanischen Programmen sind das Sperren, Verändern oder Vernichten von Informationen sowie das Hervorrufen von Funktionsstörunge in Computern oder Computernetzwerken. Außerdem können trojanische Program Dateien empfangen oder senden, Dateien ausführen, auf dem Bildschirm Meldunge anzeigen, auf Webseiten zugreifen, Programme herunterladen und installieren, und einen Computer neu starten.

Häufig verwenden Angreifer eine „Kombination" aus unterschiedlichen Trojanerprogrammen.

Die folgende Tabelle unterscheidet die Typen der trojanischen Programme nach ihrem Verhalten.

Typen der trojanischen Programme nach ihrem Verhalten auf einem infizierten Computer

Typ	Name	Beschreibung
Trojan-ArcBomb	Trojanische Programme – „Archivbomben"	Archive. Beim Extrahieren vergrößert sich der Inhalt so stark, dass es auf dem Computer zu Funktionsstörungen kommt. Wenn der Benutzer versucht, ein solches Archiv zu entpacken, kann es sein, dass die Leistung des Computers sinkt, der Computer hängen bleibt oder die Festplatte mit „leeren" Daten überfüllt wird. Eine besondere Gefahr bilden „Archivbomben" für Datei- und Mailserver. Wird auf dem Server ein System zur automatischen Verarbeitung eingehender Daten verwendet, kann eine „Archivbombe" den Server zum Absturz bringen.
Backdoor	Trojanische Programme zur Remote-Administration	Dieser Typ gilt unter den trojanischen Programmen als der gefährlichste. Sie gleicher funktionsmäßig Programmen, die zur Remote-Administration auf einem Computer installiert werden.

		Diese Programme installieren sich auf dem Computer, ohne dass der Benutzer etwas davon bemerkt, und ermöglichen dem Angreifer die Fernsteuerung des Computers.
Trojan	Trojanische Programme	Dieser Typ umfasst folgende schädlichen Programme: • **Klassische trojanische Programme**. Diese Programme führen nur die Grundfunktionen trojanischer Programme aus: Sperrung, Veränderung oder Zerstörung von Informationen, Störung der Arbeit von Computern oder Computernetzwerken. Sie besitzen keine Zusatzfunktionen, über die andere Trojaner-Typen verfügen, die in dieser Tabelle beschrieben sind. • **"Mehrzweck"-Trojaner**. Sie besitzen Zusatzfunktionen, die gleichzeitig für mehrere Typen trojanischer Programme charakteristisch sind.
Trojan-Ransom	Trojanische Erpressungsprogramme	Sie nehmen die Daten auf einem PC als „Geisel", indem sie diese verändern oder sperren, oder stören die Arbeit des Computers, damit der Benutzer nicht mehr auf seine Daten zugreifen kann. Der Angreifer fordert vom Benutzer ein Lösegeld und verspricht, dafür ein Programm zu liefern, das die Funktionsfähigkeit des Computers und der Daten wiederherstellt.
Trojan-Clicker	Trojanische Clicker-Programme	Diese Programme greifen von einem PC aus auf Webseiten zu: Sie senden entweder selbst Befehle an den Browse oder ersetzen Webadressen, die in Systemdateien gespeichert sind.

		Mithilfe dieser Programme organisieren Angreifer Netzwerkangriffe oder steigern die Besucherzahlen von Seiten, um die Anzeigehäufigkeit von Werbebannern zu erhöhen.
Trojan-Downloader	Trojanische Download-Programme	Sie greifen auf die Webseite des Eindringlings zu, laden von dort andere bösartige Programme herunter und installieren sie auf dem Computer des Benutzers. Sie können den Dateinamen des böswilligen Programms enthalten, die heruntergeladen oder von der Webseite, auf die zugegriffen wird, empfangen werden soll.
Trojan-Dropper	Trojanische Installationsprogramme	Nachdem sie auf der Computerfestplatte gespeichert wurden, installieren sie andere trojanische Programme, die sich in ihrem Körper befinden. Angreifer können trojanische Installationsprogramme zu folgenden Zwecken verwenden: • um ohne Wissen des Benutzers ein schädliches Programm zu installieren: Trojanische Installationsprogramme zeigen keinerlei Meldungen an oder blenden falsche Meldungen über einen Fehler im Archiv oder eine inkorrekte Version des Betriebssystems ein. • um andere bekannte Schadsoftware vor der Entdeckung zu schützen: Nicht alle Antiviren-Programme können Schadsoftware in trojanischen Installationsprogrammen erkennen.
Trojan-Notifier	Trojanische Benachrichtigungsprogramme	Sie informieren einen Angreifer darüber, dass der infizierte Computer „online“ ist und übermitteln folgende Informationen über den Computer: IP-Adresse,

		Nummer des offenen Ports oder E-Mail-Adresse. Sie nehmen per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise Kontakt mit dem Angreifer auf. Trojanische Benachrichtigungsprogramme werden häufig in Kombination mit unterschiedlichen Trojanerprogrammen eingesetzt. Sie teilen dem Angreifer mit, dass andere trojanische Programme erfolgreich auf einem PC installiert wurden.
Trojan-Proxy	Trojanische Proxy-Programme	Sie ermöglichen es einem Angreifer, über einen PC anonym auf Webseiten zuzugreifen. Sie dienen häufig zum Spam-Versand.
Trojan-PSW	Trojanische Programme zum Kennwortdiebstahl	Trojanische Programme, die Kennwörter stehlen (Password Stealing Ware). Sie berauben Benutzerkonten und stehlen beispielsweise Registrierungsdaten für Softwareprodukte. Sie durchsuchen Systemdateien und die Registrierung nach vertraulichen Daten und schicken diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. Einige dieser trojanischen Programme werden speziellen Typen zugeordnet, die in dieser Tabelle beschrieben sind. Dazu zählen Trojaner, die Bankkonten berauben (Trojan-Banker), Daten von IM-Clients stehlen (Trojan-IM) und Daten aus Netzwerkspielen entwenden (Trojan-GameThief).
Trojan-Spy	Trojanische Spyware-Programme	Sie spionieren den Benutzer aus und sammeln Informationen über die Aktionen, die der Benutzer bei der Arbeit am Computer ausführt. Sie können die Daten abfangen, die der Benutzer über die Tastatur eingibt, Screenshots machen

		oder Listen aktiver Programme sammeln. Die gesammelten Informationen werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-DDoS	Trojanische Programme für Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung). Häufig werden mehrere Computer von solchen Programmen infiziert, um sie dann gleichzeitig für einen gezielten Angriff auf einen Server zu verwenden. DoS-Programme realisieren einen Angriff von einem Computer aus, wobei der Benutzer davon weiß. DDoS-Programme (Distributed DoS) verwenden eine größere Anzahl von Computern ohne Wissen der Benutzer für verteilte Angriffe.
Trojan-IM	Trojanische Programme zum Diebstahl der Daten von IM-Client-Benutzern	Sie stehlen Nummern und Kennwörter der Benutzer von IM-Clients. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Rootkit	Rootkits	Sie maskieren andere bösartige Programme und deren Aktivität und verlängern so die Persistenz der Programme im Betriebssystem. Sie können auch Dateien, Prozesse im Speicher eines infizierten Computers oder Registrierungsschlüssel, die bösartige Programme ausführen, verbergen. Die Rootkits können den Datenaustausch zwischen Programmen auf dem Computer des Benutzers und

		anderen Computern im Netzwerk maskieren.
Trojan-SMS	Trojanische Programme für SMS-Nachrichten	Sie infizieren Handys und versenden SMS-Nachrichten an kostenpflichtige Nummern.
Trojan-GameThief	Trojanische Programme zum Diebstahl von Benutzerdaten aus Netzwerkspielen	Sie stehlen Kontodaten von Benutzern, die an Netzwerkspielen für Computer teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Banker	Trojanische Programme zum Diebstahl von Daten über Bankkonten	Sie stehlen Daten über Bankkonten oder über Konten bei elektronischen Zahlungssystemen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Mailfinder	Trojanische Programme, die E-Mail-Adressen sammeln	Sie sammeln auf einem Computer E-Mail-Adressen und übermitteln diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. An die gesammelten Adressen kann der Angreifer Spam verschicken.

- Schädliche Tools

Subkategorie: schädliche Tools (Malicious_tools)

Gefahrenstufe: mittel

Im Gegensatz zu anderen Arten von Malware führen bösartige Tools ihre Aktionen nicht sofort nach dem Start aus. Sie können auf dem Computer des Benutzers sicher gespeichert und gestartet werden. Angreifer verwenden die Funktionen dieser Programme, um Viren, Würmer und Trojaner zu erstellen, Netzwerkangriffe gegen Remote-Server zu organisieren, Computer zu „hacken“ und andere schädlic Aktionen durchzuführen.

Die folgende Tabelle kategorisiert die unterschiedlichen Funktionen von schädliche Tools.

Funktionen von schädlichen Tools

Typ	Name	Beschreibung
Constructor	Konstrukteure	Mit ihrer Hilfe können neue Viren, Würmer und trojanische Programme erstellt werden. Einige Konstrukteure verfügen über eine standardmäßige Fensteroberfläche, in der über ein Menü der Typ einer zu erstellenden Schadsoftware, die Methode zur Debugger-Abwehr und sonstige Eigenschaften gewählt werden.
Dos	Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung).
Exploit	Exploits	Exploits bestehen aus einer Datenkombination oder aus Programmcode, der die Schwachstellen eines Programms, in dem er verarbeitet wird, ausnutzt, um auf dem Computer eine schädliche Aktion auszuführen Ein Exploit kann beispielsweise Dateien schreiben oder lesen oder auf „infizierte“ Webseiten zugreifen.

		Es gibt verschiedene Arten von Exploits, die Schwachstellen unterschiedlicher Programme oder Netzwerkdienste ausnutzen. Exploits werden in Form eines Netzwerkpakets über ein Netzwerk an mehrere Computer übertragen, um Computer mit anfälligen Netzwerkdiensten zu finden. Ein Exploit in einer DOC-Datei nutzt die Schwachstellen eines Textverarbeitungsprogramms. Er kann damit beginnen, die vom Angreifer programmierten Funktionen auszuführen, sobald der Benutzer eine infizierte Datei öffnet. Ein Exploit, der in eine E-Mail-Nachricht eingebettet ist, sucht nach Schwachstellen in einem Mail-Client. Er kann mit der Ausführung einer schädlichen Aktion beginnen, sobald der Benutzer die infizierte E-Mail in diesem Mail-Client öffnet. Mithilfe von Exploits werden Netzwürmer (Net-Worm) verbreitet. Nuker-*Exploits*(Nuker) bestehen aus Netzwerkpaketen, die einen Computer zum Absturz bringen.
FileCryptor	Verschlüsselungsprogramme	Chiffreure verschlüsseln schädliche Programme, um sie vor Antiviren-Programmen zu verstecken.
Flooder	Programme zur „Verunreinigung“ von Netzwerken	Sie versenden eine hohe Anzahl von Nachrichten über Netzwerkkanäle. Zu diesem Typ zählen beispielsweise Programme, die der Verunreinigung von Internet Relay Chats dienen. Programme, die der Verunreinigung von Kanälen für E-Mail, IM-Clients und Mobilfunksysteme dienen, zählen nicht zu diesem Typ. Diese Programme werden separaten Typen zugeordnet, die ebenfalls in dieser Tabelle beschrieben sind (Email-Flooder, IM-Flooder und SMS-Flooder).

HackTool	Hacker-Tools	Sie können die Kontrolle über den Computer, auf dem sie installiert sind, übernehmen oder einen anderen Computer angreifen (z. B. ohne Erlaubnis des Benutzers andere Systembenutzer hinzufügen und Systemberichte löschen, um ihre Spuren im System zu verwischen). Zu diesem Typ gehören bestimmte Sniffer, die über schädliche Funktionen wie z. B. das Abfangen von Kennwörtern verfügen. Sniffer (Sniffers) sind Programme, die den Netzwerkverkehr abhören können.
Hoax	Böse Scherze	Diese Programme erschrecken einen Benutzer mit virenähnlichen Meldungen: Sie zeigen fiktive Meldungen über Virenfunde in sauberen Dateien oder über das Formatieren der Festplatte an.
Spoofer	Imitator-Tools	Sie senden E-Mails und Netzwerkanfragen mit gefälschten Absenderadressen. Imitatoren werden beispielsweise von Angreifern verwendet, um einen falschen Absender vorzutäuschen.
VirTool	Tools zur Modifikation schädlicher Programme	Sie erlauben es, andere schädliche Programme so zu modifizieren, dass sie sich vor Antiviren-Programmen verstecken können.
Email-Flooder	Programme zur „Verunreinigung“ von E-Mail-Postfächern	Sie versenden eine hohe Anzahl von Nachrichten an E-Mail-Adressen (“verstopfen diese mit Müll“). Die große Menge von E-Mails hindert der Benutzer daran, erwünschte eingehende Post zu erkennen.
IM-Flooder	Programme zur „Verunreinigung“ von IM-Clients	Sie versenden eine hohe Anzahl von Nachrichten an Benutzer von IM-Clients Das hohe Nachrichtenaufkommen hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
SMS-Flooder	Programme zur „Verunreinigung“ von SMS-Systemen	Sie versenden eine große Anzahl von SMS-Nachrichten an Mobiltelefone.

- Adware

  Unterkategorie: Adware

  Bedrohungsstufe: mittel

  Adware-Programme dienen dazu, dem Benutzer Werbung zu zeigen. Sie zeigen au der Oberfläche anderer Programme Werbebanner an oder leiten Suchanfragen au Webseiten mit Werbung um. Einige von ihnen sammeln auf Werbung bezogene Informationen über den Benutzer und leiten sie an ihren Urheber weiter, z.B. Informationen darüber, welche Webseiten der Benutzer besucht und welche Suchanfragen er vornimmt. Im Gegensatz zu trojanischer Spyware leiten Adware-Programme diese Informationen mit der Erlaubnis des Benutzers weiter.

- Dialer

Unterkategorie: legale Programme, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gefahrenstufe: mittel

Die Mehrzahl dieser Programme sind nützliche Programme. Sie werden von vielen Anwendern eingesetzt. Dazu zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für die Dienste FTP, HTTP oder Telnet.

Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf eine PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Dialer	Dialer	Dialer können heimlich Telefonverbindungen über ein Modem herstellen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern.

		Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-

		Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- Erkennung von anderen Programmen, mit denen Kriminele den Computer oder die Benutzerdaten beschädigen können

Unterkategorie: legale Programme, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gefahrenstufe: mittel

Die Mehrzahl dieser Programme sind nützliche Programme. Sie werden von vielen Anwendern eingesetzt. Dazu zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für die Dienste FTP, HTTP oder Telnet.

Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf eine PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Dialer	Dialer	Dialer können heimlich Telefonverbindungen über ein Modem herstellen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern.

		Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-

		Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- **Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kan**

  Kaspersky Endpoint Security untersucht gepackte Objekte und das SFX-Modul vo selbstentpackenden SFX-Archiven (self-extracting archive).

  Angreifer packen gefährliche Programme mit speziellen Packern oder sie packen Objekte mehrfach, um sie vor Anti-Virus zu verstecken.

  Die Virenanalysten von Kaspersky haben analysiert, welche Packer am häufigsten v Angreifern eingesetzt werden.

  Erkennt Kaspersky Endpoint Security in einem Objekt einen solchen Packer, enthä dieser aller Wahrscheinlichkeit nach ein Schadprogramm oder ein Programm, das v einem Angreifer zur Schädigung des Computers oder der Daten des Benutzers verwendet werden kann.

  Kaspersky Endpoint Security erkennt folgende Programme:

  - *Gepackte Dateien, die Schaden verursachen können* – Solche Dateien dienen zum Packen von Schadprogrammen wie Viren, Würmern und Trojanern.
  - *Mehrfach gepackte Dateien* (mittlerer Bedrohungsgrad) – Dies sind Objekte, di dreimal mit einem oder mehreren Packprogrammen gepackt wurden.

- **Mehrfach gepackte Dateien**

  Kaspersky Endpoint Security untersucht gepackte Objekte und das SFX-Modul vo selbstentpackenden SFX-Archiven (self-extracting archive).

  Angreifer packen gefährliche Programme mit speziellen Packern oder sie packen Objekte mehrfach, um sie vor Anti-Virus zu verstecken.

  Die Virenanalysten von Kaspersky haben analysiert, welche Packer am häufigsten v Angreifern eingesetzt werden.

  Erkennt Kaspersky Endpoint Security in einem Objekt einen solchen Packer, enthä dieser aller Wahrscheinlichkeit nach ein Schadprogramm oder ein Programm, das v einem Angreifer zur Schädigung des Computers oder der Daten des Benutzers verwendet werden kann.

  Kaspersky Endpoint Security erkennt folgende Programme:

  - *Gepackte Dateien, die Schaden verursachen können* – Solche Dateien dienen zum Packen von Schadprogrammen wie Viren, Würmern und Trojanern.
  - *Mehrfach gepackte Dateien* (mittlerer Bedrohungsgrad) – Dies sind Objekte, di dreimal mit einem oder mehreren Packprogrammen gepackt wurden.

Ausnahmen	Diese Tabelle enthält Informationen über die Untersuchungsausnahmen.
	Objekte können wie folgt von der Untersuchung ausgeschlossen werden:
	• Geben Sie einen Datei- oder Ordnerpfad an.
	• Geben Sie den Hash eines Objekts an.
	• Verwenden Sie Masken:
	  • Zeichen `*`, das als Platzhalter für eine beliebige Zeichenkombination steht, die auc leer sein kann. Eine Ausnahme bilden die Zeichen `\` und `/` (Trennzeichen für Datei Ordnernamen in Datei- und Ordnerpfaden). Beispiel: Die Maske `C:\*\*.txt` umf alle Pfade von Dateien mit der Erweiterung txt, die sich in Ordnern auf Laufwerk C befinden, allerdings nicht in untergeordneten Ordnern.
	  • Zwei aufeinanderfolgende Zeichen `*` ersetzen in einem Datei- oder Ordnernamer beliebige Zeichenkombination. Dabei kann der Name auch leer sein und die Zeiche und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- und Ordnerpfaden) enthalten. Beispiel: Die Maske `C:\Folder\**\*.txt` umfasst alle Pfade von Dat mit der Erweiterung txt im Ordner `Folder` und in den Unterordnern. Die Maske mu mindestens eine Verschachtelungsebene umfassen. Die Maske `C:\**\*.txt` funktioniert nicht.
	  • Zeichen `?`, das als Platzhalter für ein beliebiges Einzelzeichen steht. Eine Ausnahm bilden die Zeichen `\` und `/` (Trennzeichen für Datei- und Ordnernamen in Datei- u Ordnerpfaden). Beispiel: Die Maske `C:\Folder\???.txt` umfasst die Pfade aller Dateien, die im Ordner mit dem Namen `Folder` enthalten sind, die Erweiterung TX haben und deren Name aus drei Zeichen besteht.
	• Um den Namen des Objekttyps einzugeben, verwenden Sie die Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Möglic sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) un dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Anga der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC` `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

Vertrauenswürdige Programme	Tabelle mit vertrauenswürdigen Programmen, deren Aktivität von Kaspersky Endpoint Security nicht untersucht wird. Die Komponente „Programmkontrolle“ reguliert den Start aller Programme unabhängig davon, ob ein Programm in der Tabelle der vertrauenswürdigen Programme angegeben is oder nicht.
Werte bei Vererbung zusammenfassen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dadurch wird die Liste der Untersuchungsausnahmen und vertrauenswürdigen Program den übergeordneten und untergeordneten Richtlinien von Kaspersky Security Center zusammengeführt. Um Listen zusammenzuführen, muss die untergeordnete Richtlinie so konfiguriert werden, dass sie die Einstellungen der übergeordneten Richtlinie von Kasper Security Center erbt. Wenn das Kontrollkästchen aktiviert ist, werden Listenelemente aus der übergeordneter Richtlinie von Kaspersky Security Center in untergeordneten Richtlinien angezeigt. Auf d Weise können Sie z. B. eine konsolidierte Liste der vertrauenswürdigen Programme für d gesamte Organisation erstellen.

	Vererbte Listenelemente in einer untergeordneten Richtlinie können nicht gelöscht oder bearbeitet werden. Elemente auf der Liste der Untersuchungsausnahmen und der Liste vertrauenswürdigen Programme, die während der Vererbung zusammengeführt werden, können nur in der übergeordneten Richtlinie gelöscht und bearbeitet werden. Sie können Listenelemente in untergeordneten Richtlinien hinzufügen, bearbeiten oder löschen. Wenn Elemente auf Listen der untergeordneten und übergeordneten Richtlinie übereinstimmen, werden diese Elemente als dasselbe Element der übergeordneten Rich angezeigt. Wenn das Kontrollkästchen deaktiviert ist, werden die Elemente der Listen mit vertrauenswürdigen Geräten bei der Vererbung der Einstellungen der Richtlinien für Kaspersky Security Center nicht zusammengefasst.
Verwendung lokaler Ausnahmen zulassen / Verwendung lokaler vertrauenswürdiger Programme zulassen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	*Lokale Ausnahmen und lokale vertrauenswürdige Programme (lokale vertrauenswürdige Zone)* – benutzerdefinierte Liste von Objekten und Programmen in Kaspersky Endpoint Security für einen bestimmten Computer. Kaspersky Endpoint Security überwacht keine Objekte und Programme aus der lokalen vertrauenswürdigen Zone. Auf diese Weise kön Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen. Wenn das Kontrollkästchen aktiviert ist, kann ein Benutzer eine lokale Liste von Untersuchungsausnahmen und eine lokale Liste von vertrauenswürdigen Programmen erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen. Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine List in der Richtlinie generierten Untersuchungsausnahmen und vertrauenswürdigen Progran zugreifen. Wenn eine lokale Liste erstellt wurde, schließt Kaspersky Endpoint Security na Deaktivierung dieser Funktion die aufgelisteten vertrauenswürdigen Programme weiterh von Untersuchungen aus.
Vertrauenswürdiger Zertifikatspeicher des Systems	Wenn einer der vertrauenswürdigen Zertifikatspeicher des Systems ausgewählt wird, schließt Kaspersky Endpoint Security die Programme, die mit einer vertrauenswürdigen digitalen Signatur signiert sind, von Untersuchungen aus. Kaspersky Endpoint Security w solche Programme automatisch der Gruppe *Vertrauenswürdig* zu. Wenn **Nicht verwenden** ausgewählt ist, untersucht Kaspersky Endpoint Security die Programme, unabhängig davon, ob sie eine digitale Signatur haben oder nicht. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

Programmeinstellungen

Sie können die folgenden allgemeinen Programmeinstellungen anpassen:

- Funktionsmodus
- Selbstschutz
- Leistung
- Debug-Informationen;
- Computerstatus beim Anwenden der Einstellungen

Einstellung	Beschreibung
Kaspersky Endpoint Security beim Hochfahren des Computers starten	Ist das Kontrollkästchen aktiviert, so wird Kaspersky Endpoint Security nach dem Laden des Betriebssystems gestartet und schützt den Computer während der gesamten Sitzung. Ist das Kontrollkästchen deaktiviert, so wird Kaspersky Endpoint Security nach dem Hochfahren des Betriebssystems nicht automatisch gestartet. Das Programm muss vom Benutzer manuell gestartet werden. Der Schutz des Computers ist deaktiviert, was ein Risiko für die Daten des Benutzers darstellt.
Technologie zur aktiven Desinfektion aktivieren	Wenn dieses Kontrollkästchen aktiviert ist und im Betriebssystem eine schädliche Aktivität erkannt wird, so erscheint eine Pop-up-Benachrichtigung auf dem Bildschirm. In der Benachrichtigung schlägt Kaspersky Endpoint Security vor, die aktive Desinfektion des Computers auszuführen. Wenn der Benutzer zustimmt, neutralisiert Kaspersky Endpoint Security die Bedrohung. Nach Abschluss des erweiterten Desinfektionsvorgangs startet Kaspersky Endpoint Security den Computer neu. Die Anwendung der Technologie zur aktiven Desinfektion beansprucht erhebliche Ressourcen des Computers, wodurch die Ausführung anderer Programme verlangsamt werden kann. Wenn Kaspersky Endpoint Security auf einem Computer mit Windows für Server installiert ist, zeigt Kaspersky Endpoint Security keine Benachrichtigung an. Deshalb kann der Benutzer keine Aktion zur Desinfektion einer aktiven Bedrohung auswählen. Um eine Bedrohung zu desinfizieren, müssen Sie die Technologie zur aktiven Desinfektion aktivieren in den Programmeinstellungen und Aktive Desinfektion sofort ausführen in den Aufgabeneinstellungen der *Virenuntersuchung*. Dann müssen Sie die Aufgabe *Virenuntersuchung* starten.
Kaspersky Security Center als Proxyserver für die Aktivierung verwenden *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn dieses Kontrollkästchen aktiviert ist, wird Kaspersky Security Center bei der Programmaktivierung als Proxyserver verwendet.
Selbstschutz aktivieren	Ist das Kontrollkästchen aktiviert, so verhindert Kaspersky Endpoint Security, dass Dateien des Programms auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.
Verwaltung der Einstellungen für Kaspersky Endpoint Security über Fernverwaltungsprogramme erlauben	Wenn das Kontrollkästchen aktiviert ist, können vertrauenswürdige Programme zur Remote-Administration (wie TeamViewer, LogMeIn Pro und Remotely Anywhere) die Einstellungen von Kaspersky Endpoint Security ändern. Nicht vertrauenswürdige Programme zur Remote-Administration dürfen die Einstellungen von Kaspersky Endpoint Security nicht ändern, selbst wenn das Kontrollkästchen aktiviert ist.
Externe Dienststeuerung aktivieren	Ist das Kontrollkästchen aktiviert, so erlaubt Kaspersky Endpoint Security, dass Programmdienste von einem Remote-Computer aus verwaltet werden. Wenn versucht wird, die Programmdienste von einem Remote-Computer aus fernzusteuern, erscheint eine entsprechende

	Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).
Geplante Aufgaben bei Akkubetrieb aufschieben	Ist das Kontrollkästchen aktiviert, ist der Modus zur Schonung des Akkus aktiv. Kaspersky Endpoint Security schiebt geplante Aufgaben auf. Bei Bedarf können Sie die Untersuchungs- und Update-Aufgaben manuell starten.
Ressourcen für andere Programme freigeben	Wenn Kaspersky Endpoint Security geplante Aufgaben ausführt, kann sich die Last auf den Hauptprozessor und die Laufwerkssubsysteme erhöhen, wodurch die Arbeit anderer Programme verlangsamt wird. Ist das Kontrollkästchen aktiviert, so unterbricht Kaspersky Endpoint Security bei erhöhter Last die Ausführung geplanter Aufgaben und gibt Betriebssystemressourcen für andere Programme frei.
Dump-Aufzeichnung aktivieren	Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security Dump-Dateien, wenn das Programm abstürzt. Ist das Kontrollkästchen deaktiviert, so erstellt Kaspersky Endpoint Security keine Dump-Dateien. Das Programm löscht Speicherabbilder, die bereits auf der Festplatte des Computers vorhanden sind.
Schutz für Dump-Dateien und Protokolldateien aktivieren	Ist das Kontrollkästchen aktiviert, so besitzen folgende Personen Zugriff auf Dump-Dateien: Systemadministrator und lokaler Administrator, und der Benutzer, der die Aufzeichnung von Dump- und Protokolldateien aktiviert hat. Zugriff auf Protokolldateien besitzen nur der Systemadministrator und der lokale Administrator. Ist dieses Kontrollkästchen deaktiviert, so besitzen beliebige Benutzer Zugriff auf Dump-Dateien und Protokolldateien.
Computerstatus beim Anwenden der Einstellungen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Einstellungen für die Anzeige von Statusvarianten der Client-Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist. Diese Statusvarianten werden in „Web Console“ angezeigt, wenn Fehler bei der Anwendung einer Richtlinie oder bei der Aufgabenausführung auftreten. Statusvarianten: *OK*, *Warnung* und *Kritisch*.

Berichte und Speicher

Berichte

In den Berichten werden protokolliert: Informationen über Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

Die Berichte werden im Ordner `C:\ProgramData\Kaspersky Lab\KES\Report` gespeichert.

Datenverwaltung

Das *Backup* ist ein Speicher für Backup-Kopien von Dateien, die bei der Desinfektion verändert oder gelöscht wurden. Eine *Backup-Kopie* ist die Kopie einer Datei, die vor der Desinfektion oder dem Löschen dieser Datei angelegt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Backup-Kopien von Dateien werden im Ordner `C:\ProgramData\Kaspersky Lab\KES\QB` gespeichert.

Vollständige Zugriffsrechte auf diesen Ordner besitzen die Benutzer der Gruppe „Administratoren“. Beschränkte Zugriffsrechte für diesen Ordner besitzt der Benutzer, unter dessen Benutzerkonto die Installation von Kaspersky Endpoint Security ausgeführt wurde.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Einstellungen für Berichte und Speicher

Einstellung	Beschreibung
Berichte speichern für maximal n Tage	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Berichte durch das festgelegte Zeitintervall beschränkt. Die maximale Speicherdauer für Berichte beträgt standardmäßig 30 Tage. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Dateigröße n MB	Ist das Kontrollkästchen aktiviert, so ist die maximale Größe der Berichtsdatei durch den festgelegten Wert beschränkt. Die maximale Dateigröße beträgt standardmäßig 1024 MB. Nach Erreichen der maximalen Berichtsdateigröße löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.
Objekte speichern für maximal n Tage	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Dateien durch das festgelegte Zeitintervall beschränkt. Die maximale Speicherdauer für Dateien beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.
Begrenzen der Backup-Größe auf n MB	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 100 MB. Nach Erreichen der maximalen Backup-Größe löscht Kaspersky Endpoint Security automatisch die ältesten Dateien. Dadurch ist gewährleistet, dass die maximale Backup-Größe nicht überschritten wird.
Datenübertragung an den Administrationsserver *(nur in Kaspersky Security Center verfügbar)*	Kategorien für Ereignisse auf den Client-Computern, über die Informationen an den Administrationsserver übertragen werden sollen.

Netzwerkeinstellungen

Sie können die Proxyserver-Einstellungen für die Internetverbindung und das Update der Antiviren-Datenbanken anpassen, einen Modus für die Kontrolle von Netzwerkports auswählen und die Untersuchung verschlüsselter Verbindungen anpassen.

Einstellung	Beschreibung
Datenverkehr bei getakteter Verbindung beschränken	Wenn dieses Kontrollkästchen aktiviert ist, beschränkt das Programm selbstständig den Netzwerkverkehr, wenn das Limit für die Verbindungskosten mit dem Internet erreicht wurde. Kaspersky Endpoint Security betrachtet eine Hochgeschwindigkeits-Internetverbindung als getaktet. Eine WLAN-Verbindung gilt als nicht getaktet. Cost-Aware Networking funktioniert auf Computern mit Windows 8 oder höher.
Skript für die Interaktion mit Webseiten in den Datenverkehr einbinden	Wenn dieses Kontrollkästchen aktiviert ist, bindet Kaspersky Endpoint Security ein Skript in den Datenverkehr ein, das der Interaktion mit Webseiten dient. Dieses Skript stellt sicher, dass die Web-Kontrolle-Komponente korrekt arbeiten kann. Das Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen. Ohne dieses Skript können Sie die Überwachung der Internet-Aktivitäten der Benutzer nicht aktivieren. Kaspersky-Experten empfehlen, dieses Webseiten-Interaktionsskript in den Datenverkehr einzuspeisen, um den korrekten Betrieb der Web-Kontrolle zu gewährleisten.
Proxyserver	Proxyserver-Einstellungen für den Internetzugriff durch die Benutzer von Client-Computern. Kaspersky Endpoint Security verwendet diese Einstellungen für bestimmte Schutzkomponenten und auch für das Update der Datenbanken und Programm-Module. Um einen Proxyserver automatisch anzupassen, verwendet Kaspersky Endpoint Security das WPAD-Protokoll (Web Proxy Auto-Discovery Protocol). Wenn die IP-Adresse des Proxyservers mit diesem Protokoll nicht ermittelt werden kann, verwendet Kaspersky Endpoint Security die Proxyserver-Adresse, die in den Einstellungen des Browsers Microsoft Internet Explorer angegeben ist.
Für lokale Adressen keinen Proxyserver verwenden	Ist dieses Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security keinen Proxyserver, wenn ein Update aus einem gemeinsamen Ordner erfolgt.
Kontrollierte Ports	**Alle Netzwerkports überwachen**. In diesem Modus für die Kontrolle von Netzwerkports überwachen die Schutzkomponenten (“Schutz vor bedrohlichen Dateien“, „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“) die Datenströme, die über beliebige offene Netzwerkports des Computers übertragen werden. **Nur ausgewählte Netzwerkports überwachen**. In diesem Überwachungsmodus für Netzwerkports kontrollieren die Schutzkomponenten die ausgewählten Ports des Computers und die Netzwerkaktivität der ausgewählten Programme. Eine Liste der Netzwerkports, über die E-Mail-Nachrichten und Netzwerkverkehr gewöhnlich übertragen werden, ist gemäß der Empfehlungen der Kaspersky-Experten vorgegeben. **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen**. Es wird eine vordefinierte Liste mit Programmen verwendet, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden. Diese Liste enthält z. B. Google Chrome, Adobe Reader, Java und andere Programme. **Alle Ports für die angegebenen Programme überwachen**. Es wird eine Liste mit Programmen verwendet, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden.
Untersuchung	Kaspersky Endpoint Security untersucht den verschlüsselten Netzwerkverkehr, der

verschlüsselter Verbindungen	über die folgenden Protokolle übertragen wird: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security unterstützt die folgenden Untersuchungsmodi für verschlüsselte Verbindungen: • **Verschlüsselte Verbindungen nicht untersuchen** Kaspersky Endpoint Security hat keinen Zugriff auf Inhalte von Websites, deren Adressen mit `https://` beginnen. • **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor bedrohlichen Dateien“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ angefordert wird. • **Verschlüsselte Verbindungen immer untersuchen** Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind. Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.
Beim Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat	• **Erlauben**. Ist diese Variante ausgewählt und es erfolgt ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat, so erlaubt Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite enthält eine Warnung und Informationen über den Grund, aus welchem ein Besuch dieser Domäne als riskant gilt. Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. Nach Klick auf diesen Link zeigt Kaspersky Endpoint Security eine Stunde lang keine Warnungen über ein nicht vertrauenswürdiges Zertifikat an, wenn zu anderen Ressourcen in derselben Domäne gewechselt wird. • **Verbindung blockieren** Ist diese Variante ausgewählt und es erfolgt ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat, so blockiert Kaspersky Endpoint Security die Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite informiert über den Grund, aus dem der Wechsel zu dieser Domäne blockiert wurde.

Beim Auftreten von Fehlern bei der Untersuchung verschlüsselter Verbindungen	• **Verbindung blockieren** Wenn dieses Element ausgewählt wurde und bei der Untersuchung einer geschützten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security diese Netzwerkverbindung. • **Domäne zu Ausnahmen hinzufügen**. Wenn dieses Element ausgewählt ist und bei der Untersuchung einer geschützten Verbindung ein Fehler auftritt, so fügt Kaspersky Endpoint Security die betreffende Domäne zu einer Liste der Domänen mit Untersuchungsfehlern hinzu und kontrolliert den verschlüsselten Netzwerkverkehr beim Wechsel zu dieser Domäne nicht. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich. Um den Inhalt der Liste zurückzusetzen, wählen Sie das Element **Verbindung blockieren** aus.
Verbindungen über das Protokoll SSL 2.0 blockieren	Ist das Kontrollkästchen aktiviert, so blockiert Kaspersky Endpoint Security die Netzwerkverbindungen, die über das Protokoll SSL 2.0 hergestellt werden. Ist das Kontrollkästchen deaktiviert, so blockiert Kaspersky Endpoint Security die Netzwerkverbindungen, die über das SSL 2.0-Protokoll hergestellt werden, nicht und überwacht den Netzwerkverkehr, der über diese Verbindungen übertragen wird, nicht.
Geschützte Verbindung mit einer Website, die ein EV-Zertifikat verwendet, entschlüsseln	EV-Zertifikate (eng. Extended Validation Certificate) bestätigen die Authentizität von Websites und erhöhen die Sicherheit einer Verbindung. Die Browser informieren durch ein Schloss-Symbol in der Adressleiste darüber, ob eine Website ein EV-Zertifikat hat. Außerdem kann die Adressleiste des Browsers vollständig oder teilweise grüne Farbe besitzen. Ist das Kontrollkästchen aktiviert, so entschlüsselt und überwacht Kaspersky Endpoint Security die geschützten Verbindungen, die ein EV-Zertifikat verwenden. Ist das Kontrollkästchen deaktiviert, so hat Kaspersky Endpoint Security keinen Zugriff auf den Inhalt des HTTPS-Datenverkehrs. Deshalb kontrolliert das Programm den HTTPS-Datenverkehr nur nach der Adresse einer Website, z. B. `https://facebook.com`. Wenn Sie eine Website mit einem EV-Zertifikat zum ersten Mal öffnen, wird die verschlüsselte Verbindung unabhängig davon entschlüsselt, ob das Kontrollkästchen aktiviert ist oder nicht.
Vertrauenswürdige Adressen	Es wird eine Liste mit Webadressen verwendet, für die Kaspersky Endpoint Security keine Netzwerkverbindungen untersucht. Sie können einen Domänennamen oder eine IP-Adresse eingeben. Kaspersky Endpoint Security unterstützt das Symbol `*` bei der Eingabe eines Domänennamens. Kaspersky Endpoint Security unterstützt keine Masken für IP-Adressen. Beispiele: • `domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Diese Angabe schließt Subdomänen aus (z. B. `subdomain.domain.com`). • `subdomain.domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Diese Angabe schließt die Domäne `domain.com` aus.

	• `*.domain.com` – diese Angabe schließt die folgenden Adressen ein: `https://movies.domain.com`, `https://images.domain.com/page123`. Diese Angabe schließt die Domäne `domain.com` aus.
Vertrauenswürdige Programme	Liste mit Programmen, deren Aktivität von Kaspersky Endpoint Security nicht untersucht wird. Sie können die Typen der Programmaktivität auswählen, die Kaspersky Endpoint Security nicht überwachen soll (z. B. Datenverkehr nicht untersuchen). Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
Sicheren Datenverkehr in Mozilla-Programmen untersuchen *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Ist dieses Kontrollkästchen aktiviert, so untersucht Kaspersky Endpoint Security den verschlüsselten Datenverkehr im Browser Mozilla Firefox und im Mail-Client Thunderbird. Der Zugriff auf einige Websites über das HTTPS-Protokoll ist möglicherweise gesperrt. Um den Datenverkehr im Browser „Mozilla Firefox“ und im E-Mail-Client „Thunderbird“ zu untersuchen, müssen Sie die Untersuchung verschlüsselter Verbindungen aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, untersucht Kaspersky Endpoint Security den Datenverkehr im Browser „Mozilla Firefox“ und im E-Mail-Client „Thunderbird“ nicht. Kaspersky Endpoint Security verwendet das Kaspersky-Stammzertifikat, um den verschlüsselten Datenverkehr zu entschlüsseln und zu analysieren. Sie können den Zertifikatspeicher auswählen, in dem das Kaspersky-Stammzertifikat abgelegt werden soll. • **Windows-Zertifikatspeicher verwenden**. Das Kaspersky-Stammzertifikat wird zu diesem Speicher hinzugefügt, während Kaspersky Endpoint Security installiert wird. • **Zertifikatspeicher von Mozilla verwenden**. Mozilla Firefox und Thunderbird verwenden ihre eigenen Zertifikatspeicher. Wenn der Mozilla-Zertifikatspeicher ausgewählt ist, müssen Sie das Kaspersky-Stammzertifikat in den Browser-Eigenschaften manuell zu diesem Speicher hinzufügen.

Benutzeroberfläche

Sie können die Einstellungen der Programmoberfläche anpassen.

Einstellungen der Benutzeroberfläche

Einstellung	Beschreibung
Interaktion mit dem Benutzer *(nur in der Konsole von Kaspersky Security Center verfügbar)*	**Mit vereinfachter Programmoberfläche**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.

	Mit vollständiger Programmoberfläche. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an. **Ohne Programmoberfläche**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.
Benachrichtigungseinstellungen	Tabelle mit Einstellungen für die Benachrichtigungen über unterschiedliche Ereigniskategorien. Diese Ereignisse können den Betrieb einer Komponente oder des gesamten Programms sowie die Ausführung einer Aufgabe betreffen. Die Benachrichtigungen über diese Ereignisse werden von Kaspersky Endpoint Security auf dem Bildschirm angezeigt, per E-Mail gesendet oder in Protokollen gespeichert.
E-Mail-Benachrichtigungen anpassen	Einstellungen des SMTP-Servers für den Versand von Benachrichtigungen über Ereignisse, die im Programm registriert werden.
Programmstatus im Benachrichtigungsbereich anzeigen	Kategorien der Programmereignisse, bei deren Eintreten sich das Symbol von Kaspersky Endpoint Security im Infobereich der Microsoft-Windows-Taskleiste ändert (oder).
Benachrichtigungen über den Status der lokalen Antiviren-Datenbanken	Einstellungen für die Benachrichtigungen über veraltete Antiviren-Datenbanken, die vom Programm verwendet werden.
Kennwortschutz	Ist der Schalter aktiviert, so fragt Kaspersky Endpoint Security nach dem Kennwort, wenn der Benutzer versucht, einen Vorgang auszuführen, der zum Gültigkeitsbereich des „Kennwortschutzes“ gehört. Der Gültigkeitsbereich des „Kennwortschutzes“ umfasst verbotene Vorgänge (z. B. Deaktivierung von Schutzkomponenten) und Benutzerkonten, die zum Gültigkeitsbereich des „Kennwortschutzes“ gehören. Nachdem der „Kennwortschutz“ aktiviert wurde, schlägt Kaspersky Endpoint Security vor, ein Kennwort für die Ausführung von Vorgängen festzulegen.
Webressourcen des Technischen Supports *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Liste mit Links für Websites mit Informationen über den Technischen Support für das Programm Kaspersky Endpoint Security. Die hinzugefügten Links werden im Fenster **Support** der lokalen Benutzeroberfläche von Kaspersky Endpoint Security anstelle der Standardlinks angezeigt.
Nachricht an den Benutzer *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Nachricht, die im Fenster **Support** der lokalen Oberfläche von Kaspersky Endpoint Security erscheint.

Einstellungen verwalten

Sie können die aktuellen Einstellungen von Kaspersky Endpoint Security in einer Datei speichern und diese zur schnellen Konfiguration des Programms auf einem anderen Computer verwenden. Sie können auch eine Konfigurationsdatei verwenden, wenn Sie das Programm über Kaspersky Security Center 12 mit einem Installationspaket bereitstellen. Sie können die Standardeinstellungen jederzeit wiederherstellen.

Die Einstellungen für die Verwaltung der Programmkonfiguration sind nur in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar.

Einstellungen zur Verwaltung der Programmkonfiguration

Einstellungen	Beschreibung
Import	Laden der Einstellungen für die Ausführung des Programms aus Dateien im cfg-Format und ihre Anwendung.
Export	Aktuelle Einstellungen für die Ausführung des Programms in einer Datei im cfg-Format speichern.
Wiederherstellen	Sie können jederzeit die von Kaspersky empfohlenen Einstellungen für Kaspersky Endpoint Security wiederherstellen. Wenn die Einstellungen wiederhergestellt werden, wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** festgelegt.

Aufgabenverwaltung

Für die Arbeit mit Kaspersky Endpoint Security über Kaspersky Security Center können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben für einen einzelnen Client-Computer
- Gruppenaufgaben für Client-Computer, die zu Administrationsgruppen gehören
- Aufgabe für bestimmte Computer.

Sie können beliebig viele Gruppenaufgabe, Aufgaben für bestimmte Computer und lokale Aufgaben erstellen. Details über die Verwendung von Administrationsgruppen und bestimmten Computern *finden Sie in der Hilfe für Kaspersky Security Center*.

Einstellungen für die Aufgabenverwaltung

Einstellung	Beschreibung
Verwendung lokaler Aufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden die lokalen Aufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Sofern die Richtlinie keine zusätzlichen Einschränkungen festlegt, kann der Benutzer Aufgaben anpassen und starten. Das Konfigurieren eines Ausführungszeitplan ist für den Benutzer jedoch weiterhin nicht verfügbar. Der Benutzer kann Aufgaben nur manuell ausführen. Ist dieses Kontrollkästchen deaktiviert, so können lokale Aufgaben nicht verwendet werden. In diesem Modus werden lokale Aufgaben nicht nach Zeitplan gestartet. Aufgaben können auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht gestartet und geändert werden. Dies gilt auch bei Verwendung der Befehlszeile. Der Benutzer kann wie bisher die Untersuchung einer Datei oder eines Ordners starten und dazu den Punkt **Auf Viren untersuchen** im Kontextmenü der Datei oder des Ordners verwenden. Dabei wird die Untersuchungsaufgabe mit den Einstellungswerten ausgeführt, die standardmäßig für die Aufgabe zur benutzerdefinierten Untersuchung gelten.
Anzeige von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden Gruppenaufgaben auf der lokalen Programmoberfläche von Kaspersky Endpoint Security angezeigt. Der Benutzer kann auf der Benutzeroberfläche die komplette Aufgabenliste einsehen.

	Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Endpoint Security eine leere Aufgabenliste an.
Verwaltung von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer die Gruppenaufgaben starten und anhalten, die in Kaspersky Security Center festgelegt wurden. Der Benutzer kann Aufgaben auf der Benutzeroberfläche oder auf der vereinfachten Programmoberfläche starten und anhalten. Wenn das Kontrollkästchen deaktiviert ist, startet entweder Kaspersky Endpoint Security die Aufgaben automatisch nach Zeitplan oder der Administrator startet die Aufgaben manuell in Kaspersky Security Center.

Untersuchung des Computers

Die Untersuchung auf Viren ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Untersuchungen auf Viren sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden.

Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, werden nicht durch Kaspersky Endpoint Security untersucht. Es werden aber Berichtseinträge darüber erstellt, dass diese Dateien nicht untersucht wurden.

Vollständige Untersuchung

Ausführliche Untersuchung des Systems. Kaspersky Endpoint Security untersucht folgende Objekte:

- Arbeitsspeicher des Kerns
- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Bootsektoren
- Backup des Betriebssystems
- alle Festplatten und Wechseldatenträger

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Vollständige Untersuchung* zu ändern.

Um Computerressourcen zu sparen, wird empfohlen, statt der Aufgabe zur vollständigen Untersuchung die Aufgabe zur Untersuchung im Hintergrund zu starten. Dabei bleibt das Niveau des Computerschutzes unverändert.

Untersuchung wichtiger Bereiche

Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Schnelle Untersuchung* zu ändern.

Benutzerdefinierte Untersuchung

Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte. Sie können ein beliebiges Objekt aus der folgenden Liste untersuchen:

- Arbeitsspeicher des Kerns
- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Backup des Betriebssystems
- Microsoft-Outlook-Postfach
- Festplatten, Wechseldatenträger und Netzlaufwerke
- Eine beliebige ausgewählte Datei

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Modus von Kaspersky Endpoint Security, in welchem dem Benutzer keine Benachrichtigungen angezeigt werden. Die Untersuchung im Hintergrund erfordert weniger Computerressourcen als andere Untersuchungstypen (z. B. vollständige Untersuchung). In diesem Modus untersucht Kaspersky Endpoint Security die Autostart-Objekte, den Bootsektor, den Systemspeicher und die Systempartition.

Integritätsprüfung

Kaspersky Endpoint Security überprüft, ob die Programm-Module Beschädigungen oder Änderungen aufweisen.

Untersuchungseinstellungen

Einstellung	Beschreibung
Sicherheitsstufe	Kaspersky Endpoint Security kann verschiedene Gruppen von Einstellungen für die Ausführung einer Untersuchung verwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung von zusammengesetzten Dateien untersucht Kaspersky Endpoint Security zusätzlich Dateien in Mailformaten. • **Empfohlen**. Kaspersky Endpoint Security untersucht nur die Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Außerdem werden angehängte OLE-Dateien überprüft. Archive und Installationspakete werden nicht von Kaspersky Endpoint Security untersucht. • **Niedrig**. Kaspersky Endpoint Security untersucht nur neue und veränderte Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden nicht von Kaspersky Endpoint Security untersucht.

Aktion beim Fund einer Bedrohung	**Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu. **Informieren** Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu. Bevor Sie versuchen, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt Kaspersky Endpoint Security eine Sicherungskopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.
Schutzbereich	Liste der Objekte, die im Rahmen einer Untersuchungsaufgabe von Kaspersky Endpoint Security untersucht werden. Zu den Objekten innerhalb des Untersuchungsbereichs können der Kernel-Speicher, laufende Prozesse, Bootsektoren, System-Backup-Speicher, Mail-Datenbanken, Festplatte, Wechseldatenträger oder Netzlaufwerk, Ordner oder Datei gehören.
Untersuchungszeitplan	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. **Nach Zeitplan**. In diesem Startmodus für die Untersuchungsaufgabe führt Kaspersky Endpoint Security die Untersuchungsaufgabe nach einem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Übersprungene Aufgaben ausführen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security eine übersprungene Untersuchungsaufgabe, sobald dies möglich ist. Die Untersuchungsaufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Untersuchungsaufgabe ausgeschaltet war. Wenn dieses Kontrollkästchen deaktiviert ist, startet Kaspersky Endpoint Security übersprungene Aufgaben nicht. Stattdessen führt es die nächste Untersuchungsaufgabe gemäß dem aktuellen Zeitplan aus.
Nur bei Computerleerlauf ausführen	Verschiebt den Start der Untersuchungsaufgabe, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist.
Untersuchung ausführen als	Standardmäßig wird die Untersuchungsaufgabe im Namen des Benutzers ausgeführt, mit dessen Rechten Sie im Betriebssystem registriert sind. Der Schutzbereich kann Netzlaufwerke und andere Objekte enthalten, die besondere Zugriffsrechte erfordern. Sie können in den Einstellungen von Kaspersky Endpoint Security einen Benutzer angeben, der über die erforderlichen Rechte verfügt, und die Untersuchungsaufgabe unter dem Konto dieses Benutzers ausführen.
Dateitypen	Dateien ohne Erweiterung werden von Kaspersky Endpoint Security als ausführbar betrachtet. Ausführbare Dateien werden immer von Kaspersky

	Endpoint Security untersucht, unabhängig davon, welchen Dateityp Sie für die Untersuchung gewählt haben. **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Dateien nach Format untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Bevor eine Datei auf Schadcode untersucht wird, wird die interne Kopfzeile im Hinblick auf das Dateiformat analysiert (z. B. txt, doc, exe). Während der Untersuchung werden auch Dateien mit bestimmtem Dateierweiterungen gesucht. **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.
Nur neue und veränderte Dateien untersuchen	Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.
Dateien überspringen, wenn Untersuchung länger dauert als n Sek.	Beschränkt die Untersuchungsdauer für ein einzelnes Objekt. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Dateiuntersuchung ab. Dadurch lässt sich die Untersuchungsdauer reduzieren.
Archive untersuchen	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.
Programmpakete untersuchen	Dieses Kontrollkästchen aktiviert / deaktiviert die Untersuchung der Programmpakete von Drittherstellern.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Dateien in E-Mail-Formaten untersuchen	Dieser Kontrollkasten aktiviert / deaktiviert eine Funktion, mit der Kaspersky Endpoint Security Dateien in Mailformaten und Mail-Datenbanken untersucht. Das Programm untersucht nur MS Outlook, Windows Mail/Outlook Express und EML-Mail-Dateiformate vollständig und nur dann, wenn der Computer über den Mail-Client MS Outlook x86 verfügt. Ist dieses Kontrollkästchen aktiviert, zerlegt Kaspersky Endpoint Security die Mailformat-Datei und untersucht die einzelnen Komponenten (Kopfzeile, Text, Anhänge) auf Bedrohungen. Ist dieses Kontrollkästchen deaktiviert, untersucht Kaspersky Endpoint Security die Mailformat-Datei wie eine einzelne Datei.
Kennwortgeschützte Archive untersuchen	Ist dieses Kontrollkästchen aktiviert, untersucht Kaspersky Endpoint Security kennwortgeschützte Archive. Dabei erfolgt eine Kennwortabfrage, bevor Dateien untersucht werden, die in einem Archiv enthalten sind. Ist dieses Kontrollkästchen nicht aktiviert, werden kennwortgeschützte Archive bei der Untersuchung von Kaspersky Endpoint Security übersprungen.
Große zusammengesetzte Dateien nicht entpacken	Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht. Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe. Unabhängig vom Status dieses Kontrollkästchens untersucht Kaspersky Endpoint Security große Dateien, die aus Archiven extrahiert werden.

Maschinelles Lernen und Signaturanalyse	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
iSwift-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Modus von Kaspersky Endpoint Security, in welchem dem Benutzer keine Benachrichtigungen angezeigt werden. Die Untersuchung im Hintergrund erfordert weniger Computerressourcen als andere Untersuchungstypen (z. B. vollständige Untersuchung). In diesem Modus untersucht Kaspersky Endpoint Security die Autostart-Objekte, den Bootsektor, den Systemspeicher und die Systempartition. Die Untersuchung im Hintergrund wird in folgenden Fällen gestartet:

- nach dem Update der Antiviren-Datenbanken
- 30 Minuten nach dem Start von Kaspersky Endpoint Security
- alle sechs Stunden
- Wenn der Computer für fünf Minuten oder länger im Leerlauf ist (der Computer ist gesperrt oder der Bildschirmschoner ist eingeschaltet).

Die Hintergrunduntersuchung bei Inaktivität des Computers wird unterbrochen, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Computer hat in den aktiven Modus gewechselt.

  Wenn die Untersuchung im Hintergrund seit über zehn Tagen nicht mehr ausgeführt wurde, wird die Untersuchung nicht unterbrochen.

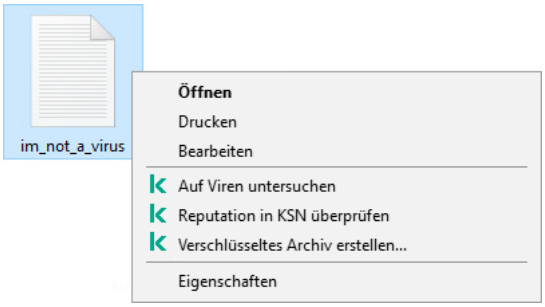
- Der Computer (das Notebook) hat in den Batteriebetrieb gewechselt.

Wenn die Aufgabe „Hintergrunduntersuchung“ ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.

Untersuchung aus dem Kontextmenü

Kaspersky Endpoint Security bietet die Möglichkeit, aus dem Kontextmenü bestimmte Dateien auf Viren und andere bedrohliche Programme zu untersuchen (s. folgende Abb.).

Wenn eine Untersuchung aus dem Kontextmenü ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.



Untersuchung aus dem Kontextmenü

Einstellungen für die Aufgabe „Untersuchung aus dem Kontextmenü“

Einstellung	Beschreibung
Aktion beim Fund einer Bedrohung	**Desinfizieren; löschen, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Schlägt die Desinfektion fehl, werden sie von Kaspersky Endpoint Security gelöscht. **Desinfizieren; blockieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Ist eine Desinfektion nicht möglich, so fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu. **Informieren** Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
Nur neue und veränderte Dateien	Untersucht nur neue Dateien und jene Dateien, die seit ihrer letzten Untersuchung verändert wurden. Dadurch lässt sich die Untersuchungsdauer reduzieren. Dieser

untersuchen	Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.
Dateien überspringen, wenn Untersuchung länger dauert als n Sek.	Beschränkt die Untersuchungsdauer für ein einzelnes Objekt. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Dateiuntersuchung ab. Dadurch lässt sich die Untersuchungsdauer reduzieren.
Archive untersuchen	Untersucht Archive der folgenden Formate: RAR, ARJ, ZIP, CAB, LHA, JAR und ICE.
Programmpakete untersuchen	Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Programmpaketen.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte.
Große zusammengesetzte Dateien nicht entpacken	Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht.
Maschinelles Lernen und Signaturanalyse	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
iSwift-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und

	kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Untersuchung von Wechseldatenträgern

Kaspersky Endpoint Security bietet eine Funktion, mit der Wechseldatenträger auf Viren und andere Schadprogramme untersucht werden können, wenn sie an den Computer angeschlossen werden.

Einstellungen für die Aufgabe „Untersuchung von Wechseldatenträgern"

Einstellung	Beschreibung
Aktion beim Anschließen eines Wechseldatenträgers	• **Nicht untersuchen** • **Detaillierte Untersuchung** Ist diese Variante ausgewählt, so untersucht Kaspersky Endpoint Security nach dem Anschließen eines Wechseldatenträgers alle Dateien, die sich auf dem Wechseldatenträger befinden, einschließlich eingebetteter Dateien in zusammengesetzten Objekten. • **Schnelle Untersuchung** Ist diese Variante ausgewählt, so untersucht Kaspersky Endpoint Security nach dem Anschließen eines Wechseldatenträgers nur Dateien mit bestimmten Formaten, die als besonders infektionsanfällig gelten. Außerdem werden zusammengesetzte Objekte nicht entpackt.
Maximale Größe des Wechseldatenträgers	Ist dieses Kontrollkästchen aktiviert, so führt Kaspersky Endpoint Security mit Wechseldatenträger, deren Größe den Höchstwert nicht überschreitet, die Aktion aus, die in der Dropdown-Liste **Aktion beim Anschließen eines Wechseldatenträgers** gewählt wurde. Ist dieses Kontrollkästchen deaktiviert, so führt Kaspersky Endpoint Security mit Wechseldatenträger die Aktion aus, die in der Dropdown-Liste **Aktion beim Anschließen eines Wechseldatenträgers** gewählt wurde, wobei die Größe der Wechseldatenträger unberücksichtigt bleibt.
Untersuchungsfortschritt anzeigen	Ist das Kontrollkästchen aktiviert, so zeigt Kaspersky Endpoint Security den Fortschritt der Untersuchung von Wechseldatenträgern in einem separaten Fenster sowie im Fenster **Aufgaben** an. Ist das Kontrollkästchen deaktiviert, so führt Kaspersky Endpoint Security die Untersuchung von Wechseldatenträgern im Hintergrundmodus aus.
Abbruch einer Untersuchungsaufgabe verbieten	Ist das Kontrollkästchen aktiviert, so sind auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security für die Aufgabe zur Untersuchung von Wechseldatenträgern die Schaltfläche **Abbrechen** im Fenster **Aufgaben** und die Schaltfläche **Beenden** im Fenster **Untersuchung auf Viren** nicht verfügbar.

Integritätsprüfung

Kaspersky Endpoint Security überprüft, ob die Programmdateien, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Beispiel: Besitzt eine Programmbibliothek eine inkorrekte digitale Signatur, so gilt diese Bibliothek als beschädigt. Zur Untersuchung von Programmdateien dient die Aufgabe *Integritätsprüfung*. Starten Sie die Aufgabe *Integritätsprüfung*, wenn das Programm Kaspersky Endpoint Security ein schädliches Objekt gefunden hat, dieses aber nicht neutralisiert wurde.

Die Aufgabe *Integritätsprüfung* können Sie in Kaspersky Security Center 12 Web Console und in der „Verwaltungskonsole“ erstellen. Diese Aufgabe kann nicht im Programm Kaspersky Security Center Cloud Console erstellt werden.

Verletzungen der Programm-Integrität können beispielsweise in den folgenden Fällen auftreten:

- Ein schädliches Objekt hat die Dateien von Kaspersky Endpoint Security verändert. In diesem Fall führen Sie den Vorgang zur Wiederherstellung von Kaspersky Endpoint Security mit Betriebssystemmitteln aus. Starten Sie nach der Wiederherstellung eine vollständige Untersuchung des Computers und wiederholen Sie die Integritätsprüfung.
- Die digitale Signatur ist abgelaufen. In diesem Fall aktualisieren Sie Kaspersky Endpoint Security.

Einstellungen für Integritätsprüfungsaufgaben

Einstellung	Beschreibung
Untersuchungszeitplan	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. **Nach Zeitplan**. In diesem Startmodus für die Untersuchungsaufgabe führt Kaspersky Endpoint Security die Untersuchungsaufgabe nach einem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Übersprungene Aufgaben ausführen	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security eine übersprungene Untersuchungsaufgabe, sobald dies möglich ist. Die Untersuchungsaufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Untersuchungsaufgabe ausgeschaltet war. Wenn dieses Kontrollkästchen deaktiviert ist, startet Kaspersky Endpoint Security übersprungene Aufgaben nicht. Stattdessen führt es die nächste Untersuchungsaufgabe gemäß dem aktuellen Zeitplan aus.
Nur bei Computerleerlauf ausführen	Verschiebt den Start der Untersuchungsaufgabe, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist.
Ausführen als *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Standardmäßig wird die Untersuchungsaufgabe im Namen des Benutzers ausgeführt, mit dessen Rechten Sie im Betriebssystem registriert sind. Für den Zugriff auf den Installationsordner des Programms können besondere Berechtigungen erforderlich sein. Sie können in den Einstellungen von Kaspersky Endpoint Security einen Benutzer angeben, der über die erforderlichen Rechte verfügt, und die Untersuchungsaufgabe unter dem Konto dieses Benutzers ausführen.

Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Als primäre Update-Quelle für Kaspersky Endpoint Security dienen die Update-Server von Kaspersky.

Der Computer muss mit dem Internet verbunden sein, um das Update-Paket erfolgreich von den Kaspersky-Update-Servern herunterzuladen. Standardmäßig wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, müssen Sie die Proxyserver-Einstellungen konfigurieren.

Updates werden mit dem HTTPS-Protokoll heruntergeladen. Falls ein Download mit dem HTTPS-Protokoll nicht möglich ist, erfolgt der Download mit dem HTTP-Protokoll.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Endpoint Security. Der Computerschutz basiert auf Datenbanken, die Signaturen für Viren und andere bedrohliche Programme, sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und der Desinfektion von infizierten Dateien auf dem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Endpoint Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Neben den Datenbanken von Kaspersky Endpoint Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Endpoint Security, fügen neue Funktionen hinzu und optimieren vorhandene Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Update-Quelle vorliegt. Sind die Datenbanken und Programm-Module nicht aktuell, werden fehlende Teile der Updates auf dem Computer installiert.

Beim Update der Programm-Module kann auch die Kontexthilfe für das Programm aktualisiert werden.

Sind die Datenbanken stark veraltet, kann das Update-Paket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Informationen über den aktuellen Status der Datenbanken für Kaspersky Endpoint Security werden im Block **Update** im Fenster **Aufgaben** angezeigt.

Informationen über die Aktualisierungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Update-Aufgabe auftreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Einstellungen für Programmmodul und Datenbanken-Update

Einstellung	Beschreibung
Startmodus	**Automatisch**. In diesem Startmodus für die Update-Aufgabe prüft Kaspersky Endpoint Security regelmäßig, ob an der Update-Quelle ein neues Update-Paket vorliegt. Die

	Häufigkeit, mit der nach einem neuen Update-Paket gesucht wird, kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neues Update-Paket gefunden wird, lädt Kaspersky Endpoint Security es herunter und installiert die Updates auf dem Computer. **Manuell**. In diesem Startmodus für die Update-Aufgabe können Sie die Update-Aufgabe manuell starten. **Nach Zeitplan**. In diesem Startmodus für die Update-Aufgabe führt Kaspersky Endpoint Security das Update nach einem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Update-Aufgabe können Sie das Update von Kaspersky Endpoint Security auch manuell starten.
Übersprungene Aufgaben ausführen	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security eine übersprungene Update-Aufgabe, sobald dies möglich ist. Eine Update-Aufgabe wird beispielsweise übersprungen, wenn der Computer zum Startzeitpunkt einer Update-Aufgabe ausgeschaltet war. Ist das Kontrollkästchen deaktiviert, so zeichnet Kaspersky Endpoint Security keine fehlenden Update-Aufgaben auf. Stattdessen wird die nächste Update-Aufgabe gemäß dem festgelegten Zeitplan ausgeführt.
Update-Quelle	Eine *Update-Quelle* ist eine Ressource, die Updates der Datenbanken und der Programm-Module für Kaspersky Endpoint Security enthält. Zu den Update-Quellen gehören der Kaspersky-Security-Center-Server, die Kaspersky-Update-Server sowie Netzwerkordner und lokale Ordner. Standardmäßig enthält die Liste für Update-Quellen den Server von Kaspersky Security Center und die Kaspersky-Update-Server. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden. Kaspersky Endpoint Security unterstützt keine Updates von HTTPS-Servern, außer es sind Kaspersky-Update-Server. Wurden mehrere Ressourcen als Update-Quellen gewählt, greift Kaspersky Endpoint Security bei einer Aktualisierung streng der Reihe nach darauf zu. Bei der Update-Aufgabe wird das Update-Paket aus der ersten verfügbaren Update-Quelle verwendet.
Aufgabe starten mit Rechten des folgenden Benutzers	Die Update-Aufgabe für Kaspersky Endpoint Security wird standardmäßig im Namen des Benutzers gestartet, mit dessen Rechten Sie sich im Betriebssystem angemeldet haben. Das Update für Kaspersky Endpoint Security kann aber auch aus einer Update-Quelle erfolgen, für welche der Benutzer keine Zugriffsrechte besitzt (z. B. aus einem gemeinsamen Ordner, welcher das Update-Paket enthält) oder für welche die Verwendung der Authentifizierung auf dem Proxyserver nicht angepasst ist. Sie können in den Einstellungen für Kaspersky Endpoint Security einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Update-Aufgabe für Kaspersky Endpoint Security im Namen dieses Benutzers starten.
Updates für Programm-Module herunterladen	Dieses Kontrollkästchen aktiviert / deaktiviert den Download von Updates für die Programm-Module zusammen mit den Updates für die Programm-Datenbanken. Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer über verfügbare Updates für Programm-Module und aktualisiert im Verlauf von Update-Vorgängen die Programm-Module. Updates für die Programm-Module werden dabei nach folgenden Einstellungen angewendet: • **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates,

	nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. • **Nur bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard. Wenn dieses Kontrollkästchen nicht aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer nicht über verfügbare Updates für Programm-Module und aktualisiert die Programm-Module im Verlauf von Update-Vorgängen nicht. Falls für ein Programm-Modul-Update zuerst ein Lizenzvertrag gelesen und bestätigt werden muss, dann installiert das Programm das Update erst nach der Zustimmung zum Lizenzvertrag. Dieses Kontrollkästchen ist standardmäßig aktiviert.
Updates in folgenden Ordner kopieren	Ist das Kontrollkästchen aktiviert, so kopiert Kaspersky Endpoint Security das Update-Paket in den gemeinsamen Ordner, der unter dem Kontrollkästchen angegeben ist. Anschließend können die übrigen Computer des lokalen Netzwerks das Update-Paket aus dem gemeinsamen Ordner herunterladen. Dadurch lässt sich Internet-Datenverkehr einsparen, da das Update-Paket nur einmal heruntergeladen werden muss. Standardmäßig ist folgender Ordner festgelegt: `C:\ProgramData\Kaspersky Lab\KES\Update distribution\`.
Proxyserver für Updates *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Proxyserver-Einstellungen für den Internetzugang der Benutzer von Client-Computern zum Update von Programmmodulen und Datenbanken. Um einen Proxyserver automatisch anzupassen, verwendet Kaspersky Endpoint Security das WPAD-Protokoll (Web Proxy Auto-Discovery Protocol). Wenn die IP-Adresse des Proxyservers mit diesem Protokoll nicht ermittelt werden kann, verwendet Kaspersky Endpoint Security die Proxyserver-Adresse, die in den Einstellungen des Browsers Microsoft Internet Explorer angegeben ist.
Für lokale Adressen keinen Proxyserver verwenden *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Ist dieses Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security keinen Proxyserver, wenn ein Update aus einem gemeinsamen Ordner erfolgt.

Anhang 2. Sicherheitsgruppen für Programme

Alle Programme, die auf dem Computer gestartet werden, werden von Kaspersky Endpoint Security in Sicherheitsgruppen eingeteilt. Die Programme werden in Sicherheitsgruppen eingeteilt. Die Einteilung erfolgt nach dem Grad der Bedrohung, die von den jeweiligen Programmen für das Betriebssystem ausgeht.

Es existieren folgende Sicherheitsgruppen:

- **Vertrauenswürdig**. Die Programme, die zu dieser Gruppe gehören, erfüllen eine oder mehrere der folgenden Bedingungen:
  - Die Programme haben die digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält Einträge über die Programme.
  - Der Benutzer hat die Programme in die Gruppe „Vertrauenswürdig“ verschoben.

  Für diese Programme gibt es keine verbotenen Vorgänge.
- **Schwach beschränkt**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat die Programme in die Gruppe „Schwach beschränkt“ verschoben.

  Für diese Programme gelten minimale Einschränkungen im Hinblick auf Betriebssystemressourcen.
- **Stark beschränkt**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat die Programme in die Gruppe „Stark beschränkt“ verschoben.

  Für diese Programme gelten erhebliche Einschränkungen im Hinblick auf Betriebssystemressourcen.
- **Nicht vertrauenswürdig**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat die Programme in die Gruppe „Nicht vertrauenswürdig“ verschoben.

  Für solche Programme sind alle Vorgänge verboten.

Anhang 3. Dateierweiterungen für die schnelle Untersuchung von Wechseldatenträgern

com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

exe – ausführbare Datei, selbstextrahierendes Archiv;

sys – Systemdatei von Microsoft Windows;

prg – Text des Programms dBase™, Clipper oder Microsoft Visual FoxPro®, Programm des Pakets WAVmaker

bin – Binärdatei

bat – Batchdatei

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

dpl – komprimierte Bibliothek für Borland Delphi

dll – Dynamic Link Library

scr – Bildschirmschonerdatei für Microsoft Windows

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

tsp – Programm, das im Timesharing-Modus arbeitet

drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic®-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer®;

asp – Active Server Pages-Skript;

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

eml – E-Mail-Nachricht für Microsoft Outlook Express

nws – neue E-Mail-Nachricht für Microsoft Outlook Express

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD®-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave® Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint®, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access®, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

Anhang 4. Dateitypen für die Anlagenfilterung im „Schutz vor E-Mail-Bedrohungen"

Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das die Dateierweiterung angibt.

Wenn Sie die Anlagenfilterung für E-Mail-Nachrichten aktiviert haben, kann die Komponente „Schutz vor E-Mail-Bedrohungen" bei der Filterung Dateien mit folgenden Erweiterungen umbenennen oder löschen:

com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

exe – ausführbare Datei, selbstextrahierendes Archiv;

sys – Systemdatei von Microsoft Windows;

prg – Text des Programms dBase™, Clipper oder Microsoft Visual FoxPro®, Programm des Pakets WAVmaker

bin – Binärdatei

bat – Batchdatei

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

dpl – komprimierte Bibliothek für Borland Delphi

dll – Dynamic Link Library

scr – Bildschirmschonerdatei für Microsoft Windows

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

tsp – Programm, das im Timesharing-Modus arbeitet

drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic®-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer®;

asp – Active Server Pages-Skript;

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

eml – E-Mail-Nachricht für Microsoft Outlook Express

nws – neue E-Mail-Nachricht für Microsoft Outlook Express

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD®-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave® Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint®, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access®, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

Anhang 5. Netzwerkeinstellungen für die Interaktion mit externen Diensten

Kaspersky Endpoint Security verwendet die folgenden Netzwerkeinstellungen für die Interaktion mit externen Diensten.

Netzwerkeinstellungen

Adresse	Beschreibung
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokoll: `HTTPS` Port: `443`	Programm aktivieren

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	Datenbanken und Programm-Module aktualisieren

`downloads.upd.kaspersky.com`	• Datenbanken und Programm-Module aktualisieren

Protokoll: `HTTPS` Port: `443`	• Überprüfen, ob die Kaspersky-Server erreichbar sind. Wenn die Server nicht über System-DNS erreichbar sind, verwendet das Programm öffentliches DNS. Dadurch wird sichergestellt, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau des Computer aufrechterhalten bleibt. Kaspersky Endpoint Security verwendet die DNS-Server aus der unten angegeben Liste in der folgenden Reihenfolge: 1. Google Public DNS (8.8.8.8) 2. Cloudflare DNS (1.1.1.1) 3. Alibaba Cloud DNS (223.6.6.6) 4. Quad9 DNS (9.9.9.9) 5. CleanBrowsing (185.228.168.168)

	Anfragen, die vom Programm gesendet werden, können Adressen von Domänen und die öffentliche IP-Adresse des Benutzers enthalten, da das Programm eine TCP/UDP-Verbindung mit dem DNS-Server herstellt. Diese Informationen sind beispielsweise erforderlich, um bei Verwendung von HTTPS das Zertifikat der Webressource zu validieren. Wenn Kaspersky Endpoint Security einen öffentlichen DNS-Server verwendet, richtet sich die Datenverarbeitung nach der Datenschutzrichtlinie des entsprechenden Dienstes. Wenn Sie verhindern möchten, dass Kaspersky Endpoint Security einen öffentlichen DSN-Server verwendet, fordern Sie beim Technischen Support ein öffentliches Patch an.
`touch.kaspersky.com` Protokoll: `HTTP`	• Abrufen der vertrauenswürdigen Zeit, um die Gültigkeitsdauer des Zertifikats zu überprüfen (TLS-Verbindung). • Warnung über verweigerten Zugriff auf eine Webressource im Browser („Schutz vor Web-Bedrohungen“ und „Web-Kontrolle“)

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
	Datenbanken und Programm-Module aktualisieren

p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com Protokoll: HTTP Port: 80	
ds.kaspersky.com Protokoll: HTTPS Port: 443	Arbeiten mit dem Kaspersky Security Network
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com Protocol: Beliebig Port: 443, 1443	Arbeiten mit dem Kaspersky Security Network
click.kaspersky.com redirect.kaspersky.com Protokoll: HTTPS	Folgen Sie den Links auf der Benutzeroberfläche
crl.kaspersky.com ocsp.kaspersky.com Protokoll: HTTP Port: 80	Public Key Infrastructure (PKI)

Anhang 6. Programmereignisse im Windows-Ereignisprotokoll

Im Windows-Ereignisprotokoll werden protokolliert: Informationen über die Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

Systemaudit

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
201	Der Endbenutzer-Lizenzvertrag wurde verletzt.	✓
203	Die Lizenz ist fast abgelaufen	–
204	Die Lizenz läuft bald ab.	–
206	Die Datenbanken fehlen oder sind beschädigt	–
207	Die Datenbanken sind stark veraltet	–
208	Die Datenbanken sind veraltet	–
209	Der Autostart des Programms wurde deaktiviert	–
210	Das automatische Update wurde deaktiviert.	–
211	der Selbstschutz des Programms ist deaktiviert.	–
212	Aufgabe kann nicht ausgeführt werden.	–
213	Der Selbstschutz hat eine Aktion mit Ressourcen des Programms blockiert	–
214	Die Schutzkomponenten wurden deaktiviert	–
215	Der Computer läuft im abgesicherten Modus	–
216	Es gibt unverarbeitete Dateien	–
217	Der Bericht wurde gelöscht.	✓
218	Die Programmeinstellungen wurden geändert.	✓
219	Die Gruppenrichtlinie wurde übernommen.	✓
220	Die Gruppenrichtlinie wurde deaktiviert	–
221	Aufgabe wurde gestartet.	–
222	Die Ausführung der Aufgabe wurde abgebrochen	–
223	Die Aufgabe wurde abgeschlossen	–
224	Das Programm muss neu gestartet werden, um das Update abzuschließen	–
225	Neustart des Computers ist notwendig	✓
226	Es sind nicht alle Programmkomponenten installiert, die mit dieser Lizenz verwendet werden können	–
227	Installierte Komponenten passen zur Lizenz.	–
229	Aktivierungsfehler	✓
230	Der Reserve-Aktivierungscode ist ungültig.	–
231	Aktive Bedrohung erkannt. Aktive Desinfektion muss gestartet werden.	–
232	Der Vorgang zur aktiven Desinfektion wurde gestartet	–
233	Der Vorgang zur aktiven Desinfektion wurde abgeschlossen	–
235	Das Programm wurde gestartet.	✓
236	Das Programm wurde beendet.	✓

237	Vorherige Programmsitzung nicht ordnungsgemäß beendet.	✓
240	Die Lizenz läuft bald ab.	✓
238	Die Abonnement-Einstellungen wurden geändert.	✓
239	Das Abonnement wurde verlängert.	✓
335	Das Objekt wurde aus dem Backup wiederhergestellt.	✓
336	Das Objekt kann nicht aus dem Backup wiederhergestellt werden.	✓
245	Verarbeitung einiger BS-Funktionen deaktiviert.	✓
250	Eine verschlüsselte Verbindung wurde getrennt.	✓
708	Die Aufgabeneinstellungen wurde erfolgreich übernommen	–
335	Das Objekt wurde aus dem Backup wiederhergestellt.	✓
2000	Benutzername und Kennwort eingeben	–
2001	Eine verdächtige Netzwerkaktivität wurde erkannt	–
2020	Die Teilnahme an KSN ist aktiviert.	–
2021	Die Teilnahme an KSN ist deaktiviert	–
2022	Die KSN-Server sind verfügbar	–
2023	Die KSN-Server sind nicht verfügbar	–
2024	Das Programm funktioniert und verarbeitet Daten gemäß den entsprechenden Gesetzen, und es verwendet die passende Infrastruktur.	✓
227	Alle Programmkomponenten, die gemäß Lizenz verwendet werden können, sind installiert und funktionieren normal	–

Verhaltensanalyse

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–
307	Das Objekt wurde gelöscht	–
308	Eine Backup-Kopie des Objekts wurde erstellt	–
311	Es kann keine Backup-Kopie des Objekts erstellt werden	–
313	Löschen ist nicht möglich.	–
323	Das Objekt wird beim Neustart gelöscht.	–
329	Das Objekt wurde umbenannt	–
331	Blockiert	–
452	Der Prozess wurde beendet	–
453	Der Prozess kann nicht beendet werden	–
455	Rollback wurde ausgeführt	–
458	Registrierungswert wurde wiederhergestellt	–
459	Der Registrierungswert wurde gelöscht	–
453	Datei-/Codeausführung blockiert	–

Exploit-Prävention

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
302	Ein schädliches Objekt wurde gefunden.	–
331	Blockiert	–
455	Rollback wurde ausgeführt	–
323	Das Objekt wird beim Neustart gelöscht.	–
307	Das Objekt wurde gelöscht	–
329	Das Objekt wurde umbenannt	–
457	Datei wurde wiederhergestellt	–
458	Registrierungswert wurde wiederhergestellt	–
459	Der Registrierungswert wurde gelöscht	–

Programm-Überwachung

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
301	Das Objekt wurde verarbeitet.	–
302	Ein schädliches Objekt wurde gefunden.	–
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–
306	Das Objekt wurde desinfiziert	–
307	Das Objekt wurde gelöscht	–
308	Eine Backup-Kopie des Objekts wurde erstellt	–
310	Es kann keine Backup-Kopie des Objekts erstellt werden	–
312	Die Desinfektion ist nicht möglich	–
313	Löschen ist nicht möglich.	–
314	Das Objekt wurde nicht verarbeitet	–
315	Das Objekt wurde übersprungen.	–
317	Bearbeitungsfehler	✓
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
320	Das Objekt ist verschlüsselt	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
323	Das Objekt wird beim Neustart gelöscht.	–
324	Das Objekt wird beim Neustart desinfiziert.	–
327	Das Objekt wurde durch eine früher desinfizierte Kopie ersetzt	–
332	Informationen über das gefundene Objekt	–
335	Das Objekt wurde aus dem Backup wiederhergestellt.	–
336	Das Objekt kann nicht aus dem Backup wiederhergestellt werden.	✓
340	Objekt aus der Allow-Liste von Private KSN	✓
401	Das Programm wurde in die Gruppe für vertrauenswürdige Programme verschoben	–
402	Das Programm wurde in die beschränkte Gruppe verschoben	–
403	Die Komponente Programm-Überwachung wurde ausgelöst	–
452	Der Prozess wurde beendet	–
453	Der Prozess kann nicht beendet werden	–

Schutz vor bedrohlichen Dateien

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
302	Ein schädliches Objekt wurde gefunden.	✓
317	Bearbeitungsfehler	✓
336	Das Objekt kann nicht aus dem Backup wiederhergestellt werden.	✓
340	Objekt aus der Allow-Liste von Private KSN	✓
301	Das Objekt wurde verarbeitet.	–
306	Das Objekt wurde desinfiziert	–
307	Das Objekt wurde gelöscht	–
308	Eine Backup-Kopie des Objekts wurde erstellt	–
310	Es kann keine Backup-Kopie des Objekts erstellt werden	–
312	Die Desinfektion ist nicht möglich	–
313	Löschen ist nicht möglich.	–
314	Das Objekt wurde nicht verarbeitet	–
315	Das Objekt wurde übersprungen.	–
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
320	Das Objekt ist verschlüsselt	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
323	Das Objekt wird beim Neustart gelöscht.	–
324	Das Objekt wird beim Neustart desinfiziert.	–
325	Das Objekt wurde durch eine früher desinfizierte Kopie ersetzt	–
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–
329	Das Objekt wurde umbenannt	–
335	Das Objekt wurde aus dem Backup wiederhergestellt.	–
452	Der Prozess wurde beendet	–
453	Der Prozess kann nicht beendet werden	–
332	Informationen über das gefundene Objekt	–

Schutz vor Web-Bedrohungen

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
301	Das Objekt wurde verarbeitet.	–
302	Ein schädliches Objekt wurde gefunden.	✓
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–
317	Bearbeitungsfehler	✓
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
329	Das Objekt wurde umbenannt	–
362	Ein gefährlicher Link wurde blockiert.	✓
1201	Ein zuvor geöffneter gefährlicher Link wurde gefunden.	✓
1211	Ein zuvor geöffneter bösartiger Link wurde gefunden.	✓
363	Ein gefährlicher Link wurde geöffnet.	✓
341	Der Download des Objekts wurde verboten	–
370	Der Link steht in der Allow-Liste von Private KSN.	✓
370	Objekt aus der Allow-Liste von Private KSN	✓
332	Informationen über das gefundene Objekt	–

Schutz vor E-Mail-Bedrohungen

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
301	Das Objekt wurde verarbeitet.	–
306	Das Objekt wurde desinfiziert	–
302	Ein schädliches Objekt wurde gefunden.	✓
317	Bearbeitungsfehler	✓
340	Objekt aus der Allow-Liste von Private KSN	✓
307	Das Objekt wurde gelöscht	–
308	Eine Backup-Kopie des Objekts wurde erstellt	–
312	Die Desinfektion ist nicht möglich	–
314	Das Objekt wurde nicht verarbeitet	–
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
329	Das Objekt wurde umbenannt	–
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer beschädigen können.	–
332	Informationen über das gefundene Objekt	–

Firewall

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
601	Die Netzwerkaktivität wurde erlaubt	–
602	Die Netzwerkaktivität wurde verboten	–

Schutz vor Netzwerkbedrohungen

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
651	Ein Netzwerkangriff wurde erkannt	–

Schutz vor modifizierten USB-Geräten

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
2050	Die Tastatur ist autorisiert	–
2051	Die Tastatur ist nicht autorisiert.	✓
2052	Fehler bei der Autorisierung der Tastatur	✓

AMSI-Schutz

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
301	Das Objekt wurde verarbeitet.	–
302	Ein schädliches Objekt wurde gefunden.	✓
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–
314	Das Objekt wurde nicht verarbeitet	–
315	Das Objekt wurde übersprungen.	–
317	Bearbeitungsfehler	✓
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
320	Das Objekt ist verschlüsselt	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
1512	Das Ergebnis der Untersuchung des Objekts wurde an eine Drittanbieter-Anwendung übermittelt.	–
329	Das Objekt wurde umbenannt	–
332	Informationen über das gefundene Objekt	–
340	Objekt aus der Allow-Liste von Private KSN	✓
2200	AMSI-Anfrage wurde blockiert.	✓

Programmkontrolle

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
701	Der Programmstart wurde erlaubt.	–
702	Der Programmstart wurde verboten.	–
703	Der Programmstart wurde im Testmodus verboten	–
704	Der Programmstart wurde im Testmodus erlaubt	–
707	Fehler in den Aufgabeneinstellungen. Aufgabeneinstellungen nicht angewendet	–
710	Vor dem Start von Kaspersky Endpoint Security für Windows wurde ein verbotener Prozess gestartet.	–
708	Die Aufgabeneinstellungen wurde erfolgreich übernommen	–

Gerätekontrolle

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
801	Der Vorgang mit dem Gerät wurde erlaubt	–
802	Der Vorgang mit dem Gerät wurde verboten	–
803	Temporärer Zugriff auf das Gerät aktiviert	✓
808	Ein Dateivorgang wurde ausgeführt	–
809	Die Netzwerkverbindung wurde blockiert	–

Web-Kontrolle

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
751	Der Zugriff wurde erlaubt.	–
752	Der Zugriff wurde verweigert.	–
753	Warnung über unerwünschten Inhalt	–
754	Es wurde trotz Warnung auf unerwünschte Inhalte zugegriffen	–
751	Eine erlaubte Seite wurde geöffnet	–

Adaptive Kontrolle von Anomalien

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
501	Beschwerde über blockierte Programmaktivität	–
2201	Die Aktion des Prozesses wurde übersprungen	–
2200	Die Aktion des Prozesses wurde blockiert	✓

Virtuelle Datentresore

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
904	Fehler bei der Anwendung von Regeln zur Verschlüsselung/Entschlüsselung von Dateien	✓
912	Fehler bei der Verschlüsselung/Entschlüsselung der Datei	✓
1305	Fehler bei der Verschlüsselung/Entschlüsselung des Geräts	✓
931	Fehler beim Erstellen eines verschlüsselten Pakets	✓
951	Fehler beim Aktivieren des portablen Modus	✓
953	Fehler beim Deaktivieren des portablen Modus	✓
1311	Laden des Verschlüsselungsmoduls ist fehlgeschlagen.	✓
1340	Die Aufgabe zur Verwaltung von Authentifizierungsagenten-Konten ist fehlgeschlagen.	✓
1312	Die Richtlinie kann nicht übernommen werden.	✓
1342	Fehler beim Upgrade der Verschlüsselungsfunktionalität	✓
1343	Upgrade der Verschlüsselungsfunktion rückgängig gemacht	✓
1345	Die Installation oder das Upgrade der Treiber für die Kaspersky-Festplattenverschlüsselung im WinRE-Image ist fehlgeschlagen.	✓
1346	Die Deinstallation der Treiber für die Kaspersky-Festplattenverschlüsselung aus dem WinRE-Image ist fehlgeschlagen.	✓
1370	BitLocker-Wiederherstellungsschlüssel wurde geändert.	✓
901	Die Anwendung von Regeln zur Verschlüsselung/Entschlüsselung von Dateien wurde gestartet	–
902	Die Anwendung von Regeln zur Verschlüsselung/Entschlüsselung von Dateien wurde abgeschlossen	–
903	Die Anwendung von Regeln zur Verschlüsselung/Entschlüsselung von Dateien wurde abgebrochen.	–
905	Die Anwendung von Regeln zur Verschlüsselung/Entschlüsselung von Dateien wurde fortgesetzt.	–
910	Die Verschlüsselung/Entschlüsselung der Datei wurde gestartet.	–
911	Die Verschlüsselung/Entschlüsselung der Datei wurde abgeschlossen.	–
913	Dateiverschlüsselung wurde nicht ausgeführt, weil die Datei als Ausnahme gilt.	–
914	Die Verschlüsselung/Entschlüsselung der Datei wurde abgebrochen.	–
1301	Die Verschlüsselung/Entschlüsselung des Geräts wurde gestartet.	–
1302	Die Verschlüsselung/Entschlüsselung des Geräts wurde abgeschlossen.	–
1307	Das Gerät wurde nicht verschlüsselt.	–
1303	Die Verschlüsselung/Entschlüsselung des Geräts wurde angehalten.	–
1304	Die Verschlüsselung/Entschlüsselung des Geräts wurde fortgesetzt.	–
1309	Der Vorgang zur Verschlüsselung/Entschlüsselung des Geräts wurde in	–

	den passiven Modus umgestellt.	
1308	Der Vorgang zur Verschlüsselung/Entschlüsselung des Geräts wurde in den aktiven Modus umgestellt.	–
1306	Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt	–
940	Der Zugriff auf die Datei wurde gesperrt.	✓
950	Der portable Modus wurde aktiviert.	–
952	Der portable Modus wurde deaktiviert.	–
1330	Neues Benutzerkonto des Authentifizierungsagenten wurde erstellt.	–
1337	Benutzerkonto nicht hinzugefügt. Dieses Konto ist bereits vorhanden.	–
1338	Benutzerkonto nicht geändert. Dieses Benutzerkonto ist bereits vorhanden.	–
1339	Benutzerkonto wurde nicht gelöscht. Dieses Benutzerkonto ist bereits vorhanden.	–
1331	Das Benutzerkonto des Authentifizierungsagenten wurde gelöscht	–
1332	Das Kennwort für das Benutzerkonto des Authentifizierungsagenten wurde geändert	–
1334	Die Anmeldung im Authentifizierungsagenten ist fehlgeschlagen	–
1333	Erfolgreiche Anmeldung im Authentifizierungsagenten	–
1335	Zugriff auf die Festplatte wurde mithilfe einer Zugriffsanfrage für verschlüsselte Geräte gewährt	–
1336	Ein Versuch, mithilfe einer Zugriffsanfrage für verschlüsselte Geräte Zugriff auf die Festplatte zu erhalten, ist fehlgeschlagen	–
1310	Das Verschlüsselungsmodul wurde heruntergeladen	–
1344	Das Upgrade der vollständigen Festplattenverschlüsselung wurde mit einem Fehler abgeschlossen.	✓
1341	Die Verschlüsselungsfunktionalität wurde erfolgreich aktualisiert.	✓
1332	Das Kennwort für das Benutzerkonto des Authentifizierungsagenten wurde geändert	–

Endpoint Sensor

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
2100	Der Server für Kaspersky Anti Targeted Attack Platform ist nicht verfügbar	–
2105	Der Start der Anwendung wurde blockiert.	✓
2106	Das Öffnen des Dokuments wurde blockiert.	✓
2104	Aufgaben des Servers für Kaspersky Anti Targeted Attack Platform werden verarbeitet.	–
2103	Aufgaben vom Server für Kaspersky Anti Targeted Attack Platform werden nicht verarbeitet	–
2101	Endpoint Sensor ist mit dem Server verbunden.	–
2102	Die Verbindung mit dem Server für Kaspersky Anti Targeted Attack Platform wurde wiederhergestellt	–
2112	Alle von einem Dateiabbild oder Stream gestarteten Prozesse wurden beendet.	✓
2113	Das Programm wurde gestartet.	✓
2111	Die Datei oder der Stream wurde vom Administrator des Kaspersky Anti Targeted Attack Platform-Servers gelöscht.	✓
2110	Die Datei wurde vom Administrator aus der Quarantäne des Servers für Kaspersky Anti Targeted Attack Platform wiederhergestellt.	✓
2109	Die Datei wurde vom Administrator in die Quarantäne des Kaspersky Anti Targeted Attack Platform-Servers verschoben.	✓
2107	Eine Netzwerkaktivität von Dritthersteller-Programmen wurde blockiert.	✓
2108	Die Netzwerkaktivität aller Dritthersteller-Programme wurde freigegeben.	✓

Untersuchung des Computers

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
302	Ein schädliches Objekt wurde gefunden.	✓
335	Das Objekt wurde aus dem Backup wiederhergestellt.	✓
336	Das Objekt kann nicht aus dem Backup wiederhergestellt werden.	✓
340	Objekt aus der Allow-Liste von Private KSN	✓
301	Das Objekt wurde verarbeitet.	–
329	Das Objekt wurde umbenannt	–
306	Das Objekt wurde desinfiziert	–
307	Das Objekt wurde gelöscht	–
308	Eine Backup-Kopie des Objekts wurde erstellt	–
310	Es kann keine Backup-Kopie des Objekts erstellt werden	–
312	Die Desinfektion ist nicht möglich	–
313	Löschen ist nicht möglich.	–
314	Das Objekt wurde nicht verarbeitet	–
315	Das Objekt wurde übersprungen.	–
317	Bearbeitungsfehler	–
318	Ein Archiv wurde gefunden.	–
319	Ein gepacktes Objekt wurde gefunden.	–
320	Das Objekt ist verschlüsselt	–
321	Das Objekt ist beschädigt	–
322	Ein kennwortgeschütztes Archiv wurde gefunden	–
323	Das Objekt wird beim Neustart gelöscht.	–
324	Das Objekt wird beim Neustart desinfiziert.	–
327	Das Objekt wurde durch eine früher desinfizierte Kopie ersetzt	–
303	Es wurde ein legales Programm gefunden, mit dem Angreifer Ihren Computer oder persönliche Daten beschädigen können.	–

Integritätsprüfung

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
2002	Überprüfung der Signatur eines Systemmoduls fehlgeschlagen	–

Datenbanken-Update

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
101	Ein interner Fehler ist aufgetreten.	✓
1001	Die Update-Quelle wurde ausgewählt.	–
1002	Proxyserver ausgewählt	–
1003	Dateidownload	–
1004	Datei wurde heruntergeladen.	–
1005	Datei wurde installiert.	–
1006	Datei wurde aktualisiert.	–
1007	Wegen eines Update-Fehlers wurde das Rollback der Datei ausgeführt.	–
1008	Dateien werden aktualisiert.	–
1009	Verteilen von Updates	–
1010	Rollback der Dateien	–
1011	Fehler beim Update einer Komponente	–
1012	Fehler beim Kopieren der Updates einer Komponente	–
1013	Download-Liste wird erstellt.	–
1014	Lokaler Update-Fehler	–
1016	Der Vorgang wurde vom Benutzer abgebrochen.	–
1017	Zwei Aufgaben können nicht gleichzeitig gestartet werden	–
1018	Fehler bei der Überprüfung der Datenbanken und Programm-Module	–
1019	Fehler bei Interaktion mit Kaspersky Security Center	–
1020	Es sind keine Updates verfügbar	–
1021	Nicht alle Komponenten wurden aktualisiert	–
1022	Die Update-Verteilung wurde erfolgreich abgeschlossen	–
1023	Das Update wurde erfolgreich abgeschlossen, die Update-Verteilung ist jedoch fehlgeschlagen	–
2153	Fehler bei der Patch-Installation	–
2156	Fehler beim Patch-Rollback	–
2150	Patches werden heruntergeladen.	–
2151	Patches werden installiert.	–
2152	Der Patch wurde installiert.	–
2154	Der Patch wird rückgängig gemacht.	–
2155	Der Patch wurde rückgängig gemacht.	–

Daten löschen

Ereigniscodes

Ereignis-ID	Beschreibung	Standardmäßig aktiviert
223	Die Aufgabe wurde abgeschlossen	–
221	Aufgabe wurde gestartet.	–
222	Die Ausführung der Aufgabe wurde abgebrochen	–
2252	Das Objekt kann nicht gelöscht werden.	–
2253	Statistik der Aufgabe zum Entfernen	–
2251	Das Objekt wurde gelöscht	–

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich in der Installationsdatei des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, Reader und Shockwave sind Marken oder in den Vereinigten Staaten von Amerika und/oder in anderen Ländern eingetragene Marken von Adobe Systems Incorporated.

Apple, FireWire, iTunes und Safari sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Apple Inc.

AutoCAD ist ein Markenzeichen oder eingetragenes Markenzeichen von Autodesk, Inc. und/oder deren Tochterunternehmen und/oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Borland ist ein Markenzeichen oder ein eingetragenes Markenzeichen der Borland Software Corporation.

Android und Google Chrome sind Markenzeichen von Google, Inc.

Citrix und Citrix Provisioning Services, und XenDesktop sind Markenzeichen von Citrix Systems, Inc. und/oder deren Tochterunternehmen, und können in den USA und in anderen Ländern als Patente registriert sein.

Dell ist ein Markenzeichen von Dell, Inc. oder deren Tochterunternehmen.

dBase ist eine Marke der dataBased Intelligence, Inc.

EMC ist ein Markenzeichen oder eingetragenes Markenzeichen von EMC Corporation in den USA und/oder anderen Ländern.

Radmin ist eine eingetragene Marke von Famatech.

IBM ist eine Marke der International Business Machines Corporation, die in vielen Ländern registriert ist.

ICQ ist ein Markenzeichen und/oder eine Handelsmarke von ICQ LLC.

Intel ist eine in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marke der Intel Corporation.

IOS ist eine in den USA und in anderen Ländern eingetragene Marke von Cisco Systems, Inc. und/oder der damit verbundenen Unternehmen.

Lenovo und ThinkPad sind Markenzeichen von Lenovo in den USA und/oder anderen Ländern.

Linux ist eine in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragen Marke von Linus Torvalds.

Logitech ist eine in den Vereinigten Staaten von Amerika und (oder) in anderen Ländern eingetragene Marke oder eine Marke des Unternehmens Logitech.

LogMeIn Pro und Remotely Anywhere sind Markenzeichen von LogMeIn, Inc.

Mail.ru ist ein eingetragenes Markenzeichen von Mail.Ru, LLC.

McAfee ist ein Markenzeichen oder eingetragenes Markenzeichen von McAfee, Inc. in den USA und anderen Ländern.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface und Hyper-V sind Markenzeichen der Microsoft Corporation in den USA und anderen Ländern.

Mozilla, Firefox und Thunderbird sind Marken der Mozilla Foundation.

Java und JavaScript sind eingetragene Markenzeichen von Oracle und/oder der verbundenen Unternehmen.

VERISIGN ist ein eingetragenes Markenzeichen in den USA und anderen Ländern oder ein nicht eingetragenes Markenzeichen von VeriSign, Inc. und seinen Tochterunternehmen.

VMware и VMware ESXi sind Markenzeichen von VMware, Inc. oder in den USA und anderen Ländern eingetragene Markenzeichen von VMware, Inc.

Thawte ist ein Markenzeichen oder eingetragenes Markenzeichen der Symantec Corporation oder der verbundenen Unternehmen in den USA und anderen Ländern.

SAMSUNG ist ein Markenzeichen von SAMSUNG in den USA und anderen Ländern.